DESIGN, DEVELOPMENT AND IMPLEMENTATION OF AN INFORMATION SECURITY AND CYBERETHICS COURSE FOR PRE-SERVICE TEACHERS: A DESIGN-BASED RESEARCH

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

EVRİM AKMAN KADIOĞLU

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
COMPUTER EDUCATION AND INSTRUCTIONAL TECHNOLOGY

APRIL 2019

Approval of the thesis:

DESIGN, DEVELOPMENT AND IMPLEMENTATION OF AN INFORMATION SECURITY AND CYBERETHICS COURSE FOR PRE-SERVICE TEACHERS: A DESIGN-BASED RESEARCH

Submitted by **EVRİM AKMAN KADIOĞLU** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy** in **Computer Education and Instructional Technology Department, Middle East Technical University** by,

Prof. Dr. Halil Kalıpçılar
Dean, Graduate School of **Natural and Applied Sciences** _____

Assoc. Dr. Ömer Delialioğlu
Head of Department, **Comp. Edu. and Inst. Tech.** _____

Assist. Prof. Dr. Cengiz Savaş Aşkun
Supervisor, **Comp. Edu. and Inst. Tech., METU** _____

Examining Committee Members:

Prof. Dr. Hakan Tüzün
Comp. Edu. and Inst. Tech., Hacettepe Uni. _____

Assist. Prof. Dr. Cengiz Savaş Aşkun
Comp. Edu. and Inst. Tech., METU _____

Assoc. Prof. Dr. Ömer Delialioğlu
Comp. Edu. and Inst. Tech., METU _____

Assoc. Prof. Dr. Çiğdem Haser
Mathematics and Science Education, METU _____

Assist. Prof. Dr. Halil Ersoy
Comp. Edu. and Inst. Tech., Başkent Uni. _____

Date: 05.04.2019

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname: Evrim Akman Kadıoğlu

Signature:

ABSTRACT

DESIGN, DEVELOPMENT AND IMPLEMENTATION OF AN INFORMATION SECURITY AND CYBERETHICS COURSE FOR PRE-SERVICE TEACHERS: A DESIGN-BASED RESEARCH

Akman Kadıoğlu, Evrim
Doctor of Philosophy, Computer Education and Instructional Technology
Supervisor: Assist. Prof. Dr. Cengiz Savaş Aşkun

April 2019, 252 Pages

With the introduction of the Information and Communication Technologies (ICT) into our lives, production and distribution of information have increased exponentially. The ICT systems and the data, which these systems use, create, or both is an essential resource of schools. For this reason, the secure and ethical use of information is a primary concern for schools. However, the curriculum in teacher training institutions does not include a course that aims to raise pre-service teachers' awareness of information security and cyberethics. In other words, there is a need for more instructional content on information security and cyberethics for pre-service teachers.

The designed, developed and implemented course for this study significantly improves the amount of content for pre-service teachers' information security awareness and cyberethics sensitivity. The main purpose of this study is to explore important points of designing process of a course including such an instructional content, to enhance pre-service teachers' information security awareness and cyberethics sensitivity in the Faculty of Education.

The research questions of the study can be summarized as; (i) what are content, learner, and instruction related issues during the design and development of a course

to increase the pre-service teachers' information security awareness and cyberethics sensitivity? (ii) What are the facilitating and challenging factors faced during the implementation, and how the challenges are handled from the instructor's experience? (iii) How do pre-service teachers perceive the contribution of the course on their information security awareness and cyberethics sensitivity?

Design-Based Research (DBR) approach with qualitative methods is carried out to answer these questions. As a result of this research, a course content aimed at raising pre-service teachers' information security and cyberethics awareness presented, and critical elements in the design and development process of such a course are identified.

In the scope of the study, during the need analysis and the development phases of the study, a content pool including different cybersecurity, cyberethics, and cybersafety issues and a draft content sequence have emerged. At the end of the two iterative implementation phases, the course design has reached to the final form which included different instructional methods such as face to face lecture sessions, online discussion forums and in-class discussion sessions, reading materials, and different audiovisual materials. The qualitative data analysis shows that the course influenced the students' preferences on online activities and password protection strategies. Besides, their information security and cyberethics awareness have raised. Furthermore, daily life correspondence of the course topics facilitates the instruction process and increases the learners' interest.

Keywords: Information Security, Cyberethics, Design-Based Research, Course Design and Development, Pre-service Teachers

ÖZ

ÖĞRETMEN ADAYLARI İÇİN BİLGİ GÜVENLİĞİ VE BİLİŞİM ETİĞİ DERSİNİN TASARIM, GELİŞTİRME VE UYGULAMASI: TASARIM TEMELLİ ARAŞTIRMA

Akman Kadıoğlu, Evrim
Doktora, Bilgisayar ve Öğretim Teknolojileri Eğitimi
Tez Danışmanı: Dr. Ögr. Üyesi Cengiz Savaş Aşkun

Nisan 2019, 252 Sayfa

Bilgi ve İletişim Teknolojilerinin (BİT) hayatımıza girmesiyle, bilginin üretimi ve iletimi katlanarak artmıştır. BİT teknolojilerinin kullandığı ve/ya oluşturduğu bilgiler, eğitim kurumlarının önemli bir kaynağıdır. Bu nedenle, bilginin güvenli ve etik değerlere uygun olarak kullanılması bu kurumların önemli kaygıları arasındadır. Bununla birlikte, öğretmen yetiştiren kurumların müfredatında, öğretmen adaylarının bilgi güvenliği ve bilişim etiği farkındalığını artırmayı hedefleyen bir ders bulunmamaktadır. Diğer bir deyişle öğretmen adayları için bilgi güvenliği ve bilişim etiği hakkında daha fazla eğitim içeriğine ihtiyaç bulunmaktadır.

Öğretmen adaylarının bilgi güvenliği ve bilişim etiği farkındalığını arttırmak için bu araştırma kapsamında tasarlanan, geliştirilen ve uygulanan bu ders bilgi güvenliği ve bilişim etiği hakkındaki eğitsel içerik ihtiyacına anlamlı bir katkı sağlayacaktır. Bu araştırmanın temel kaygısı, bu içeriğe yönelik bir dersin tasarım, geliştirme ve uygulama aşamalarındaki önemli noktaları belirlemek ve öğretmen adaylarının bilgi güvenliği ve bilişim etiği farkındalıklarını arttırmaktır.

Bu doğrultuda, araştırma soruları şu şekilde belirlenmiştir: (i) Öğretmen adaylarının bilgi güvenliği bilinci ve bilişim etik duyarlılık düzeylerini yükseltmek için bir ders tasarlarken, geliştirirken ve uygularken göz önüne alınan öğrenci, içerik ve öğretim ile ilgili konular nelerdir? (ii) Öğretmen adaylarının bilgi güvenliği

farkındalığı ve bilişim etiği duyarlılığını arttırmayı amaçlayan böyle bir dersin tasarım ve uygulama sürecinde karşılaşılan kolaylıklar ve zorluklar nelerdir ve zorluklar nasıl aşılmıştır? (iii) Öğretmen adayları böyle bir dersin bilişim etik duyarlılıklarını ve bilgi güvenliği farkındalıklarına etkilerini nasıl algılamaktadır?

Bu sorulara cevap bulmak için nitel yöntemlerle Tasarım Temelli Araştırma (TTA) metodu uygulanmıştır. Bu araştırmanın sonucunda bilgi güvenliği ve bilişim etiği duyarlılığı yüksek öğretmen adayları yetiştirmeyi hedefleyen bir ders içeriği sunulmuştur.

Bu çalışma kapsamında, ihtiyaç analizi ve geliştirme aşamalarında bilişim etiği, bilişim emniyeti ve bilişim güvenliği konularına yönelik bir içerik havuzu oluşturulmuş, ardından taslak bir izlencesi hazırlanmıştır. Ardından iki ardışık uygulama döneminin sonucunda dersin yapısı olgunlaşmıştır. Bu ders çeşitli eğitsel bileşenleri içermektedir. Örneğin yüz yüze ders oturumları, sınıf içi tartışma etkinliği, çevrim içi forum sayfaları, genişletilmiş ders notları, değişik kaynaklardan yararlanılan ders içerikleri bu örneklerden bazılarıdır. Ayrıca yapılan nitel veri analizinin sonucunda bu dersin öğrencilerin çevrim içi işlemlerle ilgili davranışlarını, şifre koruma tercihlerini etkilediği, öğrencilerin bilgi güvenliği ve bilişim etiği farkındalıklarını arttırdığı gözlenmiştir. Bunun yanı sıra ders içeriklerinin günlük yaşamla uyumlu olmasının öğretmenin öğretim süreçlerini kolaylaştırdığı ve öğrencilerin derse ilgilerini arttırdığı gözlenmiştir.

Anahtar Kelimeler: Bilgi güvenliği, Bilişim etiği, Ders tasarım ve geliştirme, Tasarım temelli araştırma, Öğretmen adayları

Dedicated to the loving memory of Eyüp Hamdi Akman, my grandfather,
one of the first educators of Republic of Turkey

ACKNOWLEDGEMENTS

I am grateful for the support of my advisor Assist. Prof. Dr. Cengiz Savaş Aşkun. I would also like to thank the members of the thesis monitoring committee; Assoc. Prof. Dr. Çiğdem Haser and Assoc. Prof. Dr. Ömer Delialioğlu for their support in several phases of the study. I want to thank the final chair of my dissertation committee, Prof. Dr. Hakan Tüzün and Assist. Prof. Dr. Halil Güllü, for their valuable suggestions that helped me to complete this thesis.

I want to thank Assoc. Prof. Dr. Hanife Akar, Assoc. Dr. Umut Beşpınar, Assoc. Prof. Dr. Funda Gülay Kadıoğlu, Dr. Selma Aydın Bayram, Dr. Levent Bayram, Dr. İbrahim Çalışır, Dr. Müge Maraşlı, Emre Sezginer, and Suna Yılmaz for their suggestions and opinions during the design and development of the course. I am also grateful to all of the students of CEIT215 for their participation in this research.

I should also thank my managers, Ferdi Ayaydın and Feride Erdal for their support and my colleagues for their opinions during the implementation of the study.

Assist. Prof. Dr. Gülfidan Can and Assist. Prof. Dr. Göknur Kaplan, I would like to express my deepest gratitude for your contribution during the study. I am also grateful to Assist. Prof. Dr. Gökçe Gökalp, Assoc. Prof. Dr. Birten Çelik, Dr. Serkan Alkan, Dr. Tonguç Çağın for their coaching and encouragement throughout the writing process.

Her contribution to this study was not limited to her expertise in the subject. Since the very first day of the study, Dr. Ayşe Gül Kara Aydemir was present and willingly ready to assist me at each issue I had and about every problem I have consulted to her. If it were not for her disturbed late night sleeps and her valuable criticism, suggestions and friendship, this study could not be completed in the way it is completed.

Last but not least, no matter how much I would thank my family; I would fall short of expressing my gratitude to them for their support. My dearest Suat Kadıoğlu; Thank you very much. My lovely sons Tuna and Oğuz, if it were not for wondrous journey, when I felt alone and helpless, you were my remedy.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ADDIE : (*An instructional design approach including the steps*) Analyze, Design, Development, Implement, Evaluate

AERC : Applied Ethics and Research Center

APWG : Anti-Phishing Working Group

AUP : Acceptable Use Policy

BİT : (*Bilgi ve İletişim Teknolojileri)* Information and Communication Technologies

C3 : (*An instructional framework of*) Cyberethics, Cybersafety, and Cybersecurity

CC : Computer Center

CEIT : Department of Computer Education and Instructional Technology

CERT : Computer Emergency Response Team

CGPA : Cumulative Grade Point Average

CIA : Confidentiality, Integrity, and Availability (*The major Information Security Triad*).

CIRT **:** Computer Incident Response Team

CMS **:** Course Management System

CoHE : Council of Higher Education

DBR : Design-Based Research

DMCA : Digital Millennium Copyright Act

ECE : Department of Early Childhood Education

EME : Department of Elementary Mathematics Education

ENISA : The European Union Agency for Network and Information Security

ESE : Department of Elementary Science Education

EU : European Union

FLE : Department of Foreign Language Education

FOMO : Fear of Missing Out

FOSS : Free and Open Source Software Foundations

ICT : Information and Communications Technologies

IEC **:** International Electrotechnical Commission

IS : Information Systems

ISA : Information Security Awareness

ISO : International Standard Organization

ISO27000 : (*or* **ISO/IEC 27K**) Information Security Standards published jointly by the ISO and IEC

ISTE : International Society for Technology in Education

IT : Information Technology

ITU : The International Telecommunications Union

HSEC : Human Subject Ethics Committee

KVKK : (*Kişisel Verileri Koruma Kurumu*) Department of Privacy and Data Protection

Law 5651 : Regulation of Publications on The Internet and Combating Crimes Committed by Means of Such Publication (commonly known as "The Internet Law")

LMS : Learning Management System

MoH : Republic of Turkey Ministry of Health

MoNE : Republic of Turkey Ministry of National Education

NGO : Non-Governmental Organization

NORA : Non-Obvious Relationship Awareness

NPO : Non-Profit Organization

OS : Operating System

ÖİDB : (*Öğrenci İşleri Daire Başkanlığı*) Directorate of Student Affairs

PII : Personally Identifiable Information

RP : Rapid Prototyping

SNS : Social Networking Sites

SOME : (*Siber Olaylara Müdahale Ekibi*) Cyber Incidents Intervention Team

SW : Software

ToS : Terms of Service

TUIK : (*Türkiye İstatistik Kurumu*) Turkish Statistical Institute

USOM : (*or* **TR-CERT** – *Ulusal Siber Olaylara Müdahale Merkezi*) National Computer Emergency Response Center

CHAPTER 1.

INTRODUCTION

Throughout this chapter, the issues on information security, cybersafety and cyberethics are described. The background of the problem, the problem statement, purpose, and significance of the study, and guiding research questions are presented. Furthermore, brief information about the design of the research methodology and definitions of the concepts are also stated.

1.1. Background of the Study

With the introduction of the Information and Communication Technologies (ICT) into our lives, production and distribution of information have exponentially increased. The ICT systems and the data, which these systems use, create, or both, are the primary resources of organizations. For this reason, the secure and ethical use of information and information resources is a central concern of organizations (Al-Janabi & Al-Shourbaji, 2016; Çakır, Hava, Gülen, & Özüdoğru, 2015; Delialioglu, 2011; Gupta & Sharman, 2008; Korovessis, 2011). Information security was generally considered to be the concern of information technology (IT) employees and IT-related departments. However, the evolution of security threats on digital assets and change in the targets of these threats altered the focus of concern to the end users (Abawajy, 2014; Andersson, Reimers, & Barreto, 2014; Charest, 2013).

End users' being a target of information security threat was due to their being the weakest links in information systems (Woodhouse, 2007). Social engineering is one of the most successful security intrusions caused by the complacency of the users (Al Awawdeh & Tubaishat, 2014; ENISA, 2010; Korovessis, 2011; Mouton, Leenen, & Venter, 2016). For this reason, improving end users' information security awareness and training them as security aware and literate persons is crucial.

At this point, the questions of who should address this issue and how should it be addressed come to the forefront. Educational institutions have a critical role in raising security awareness on information security. However, research investigating information security awareness (ISA) in educational settings indicate that, the end users, either teachers or students, are not sufficiently aware of information security issues and an action to raise their awareness is necessary (Akgun & Topal, 2015; Al-Janabi & Al-Shourbaji, 2016; Çiftçi & Delialioğlu, 2016; Gokmen & Akgun, 2015).

Republic of Turkey Ministry of National Education (MoNE) published a directive concerning information and system security for users of information systems in MoNE, such as ICT tools in classrooms or online applications served to teachers or any ICT devices the teachers possess (MoNE, 2016). The directive emphasizes the general security issues; including preventing illegal contents, license issues; and technical concerns, such as password protection, backup information, and user control. MoNE also issues a circular aiming at limiting teachers' social media participation concerning the privacy of the students.

MoNE directives focus on secure and ethical behaviors of teachers when they use ICT sources. Council of Higher Education (CoHE), in line with this concern, included a course in the Department of Computer Education and Instructional Technology (CEIT) curriculum for raising the digital literacy of pre-service CEIT teachers (2018b). However, such a course has not been included in curricula of other departments of faculty of education. The objectives of the course were limited to raise the digital literacy of pre-service teachers when using computer programs, safe internet use and copyright issues.

Another critical issue is the ethical use of ICT resources. The increase in ICT tools brings ethical problems as well as information security threats. Ethical use of information systems is another concern of educational research studies. Ethics is a term that describes moral decisions (Andersson et al., 2014) of a person in his/her daily life. Cyberethics, similarly, describes the moral choices of an individual in a digital environment when using information and communication technologies (Pusey & Sadera, 2011).

Research studies aiming at investigation and increasing awareness of end users' information security, generally focus only on particular security threats such as mobile security (Allam, Flowerday, & Flowerday, 2014), phishing (Arachchilage & Love, 2014), or raising digital literacy of the end users (Farooq, Kakakhel, & Ieee, 2013). The cyberethics related studies generally focus on censorship (Mathiesen, 2009), free and/or open source software, ethical use of digital sources (Grodzinsky & Wolf, 2009; Spinello, 2008); ethical issues of interaction through social networking sites (Henderson, Auld, & Johnson, 2014), and general netiquette principles (Bynum & Rogerson, 2004; Hamiti, Reka, & Baloghová, 2014).

Cyberethics is related to information security awareness. When teacher candidates are taken into consideration, the boundaries between the concepts of information security awareness and information ethics diminish. Teachers differ from other end users in a way that, they are not only considered to be the end user of an information system, but also being a teacher, they are expected to be the role model and instructor for their students in future (Yılmaz, Şahin, & Akbulut, 2016).

1.2. Statement of the Problem

Many research studies related to information security generally focus on business or financial settings (Azari, 2003; Goodhue & Straub, 1991; Thomson & Solms, 1998). For this reason, the major motivation on users' awareness of these threats depends on financial or professional concerns. In an educational setting, on the other hand, the nature of ICT organization and the roles of end users are completely different compared to business settings. The instructors, school teachers, students, and

non-ICT administrative employees, are end users of ICT systems of an educational institution. Two main reasons cause higher education institutions' information security concern to raise; (i) managing high amount of computer resources they possess; and (ii) they provide open access to their constituents and the public (Katz, 2005). For this reason, it is especially important for higher education institutions to raise the information security awareness of the users of their ICT services.

A particularly important group of users are pre-service teachers. Because they are not only the users of ICT services themselves but also they will have the responsibility of instilling cybersecurity awareness and cyberethics concepts to their future students as well.

Different from the other occupations, teachers deal with children and teenagers, who are more vulnerable to the internet related threats such as cyberbullying (Kowalski, 2010; Sezer, Yilmaz, & Karaoglan Yilmaz, 2015), addiction (Nalwa & Anand, 2003) or malicious users (Lachman, 2013). The use of mobile devices has penetrated more among K12 students (Mert, Bülbül, & Sağıroğlu, 2012; Poll, 2015; Riola, 2014). For this reason, secure, safe and ethical use of the resources has a more critical role (Henderson et al., 2014). Teachers are responsible for ethical and secure use of information systems both for themselves and guide their students in the future. However, the curriculum of education faculties does not include a course or lectures aiming at raising the pre-service teachers' information security awareness and cyberethics sensitivity (Ben-Peretz, 1994 as cited McKenney, 2001).

The curriculum in some faculties of education includes an ICT related course which focuses on the utilization of ICT in the lectures and aiming at training computer literate pre-service teachers. The course also covers topics on cybersecurity and cyberethics. However, the recent research studies suggest that pre-service teachers are not sufficiently aware of information security (Çakır et al., 2015; Çevik & Çoban, 2016) and cyberethics (Hamiti et al., 2014; Irene & Libi, 2016; Pusey & Sadera, 2011).

So far as computing services are concerned, universities have some unique properties that distinguish them from other kinds of organizations. The network

infrastructure in universities is designed to serve the needs of not only the existing employees and students but also visitors. For example, Eduroam facility is a universal service which allows its users to access the internet in many higher education institutions at home and abroad. Besides, due to the nature of the university, the existing information in computers may include nonrenewable intellectual property that could be damaged. As routine ICT procedures, grading, registration, and students payments are critical (Misenheimer, 2014). Perez, Berry, and Hollman (2003) highlighted the actual need of awareness in an academic environment and insisted on the fact that to raise the users' awareness was the first and initial level of defense for many of the information security breaches such as virus or phishing attacks.

Although the literature emphasizes the current need of information security awareness for all components in an information system including the end users, the method of raising end users' information security awareness is generally limited to warning about password protection, or phishing treats (Tasevski, 2015). Bada and Sase (2014) concluded that these one-way awareness measures generally do not result in a change in end users security behaviors. Studies on information security awareness are more common in commercial, business and informatics settings than educational settings. Besides, training in these settings includes online static informative sites or synchronous short meetings neither of which guarantee expected change in behavior of end users'.

The definition of ISA varies in research studies. This variety is one of the main challenges in examining relevant issues. Most of the researchers agree on distinguishing awareness of information security from training and education. However, a mixing of the terms also is being used.

> *"Most definitions imply that awareness is the first level of security learning pyramid: (i) awareness aims at attracting the attention of all information system (IS) users to the security message, making them understand the importance of information security and their security obligations, and (ii) training aims at building knowledge and developing the relevant skills and*

competencies, and (iii) education aims at creating expertise (Wilson & Hash, 2003). Analyzing the relevant publications; however, it is observed that this distinction is not uniformly adopted (Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008, p. 8).”

For members of various professions, such as finance (banking) (Tse et al., 2014), communication industry (Karjalainen & Siponen, 2011), or tourism industry (Buhalis, 1998) there are different training programs. Such a training program, particularly for pre-service teachers, could not be encountered. As a result of these unclear settings, an increase in information security awareness and ethical sensitivity level of pre-service teachers is required. Pre-service teachers are not only supposed to be aware of information security issues, but also they are expected to be well trained to transfer the concepts about information security and cyberethics to their prospective students about these issues. They should also have a sense of ethical concerns both for their teaching activities in the future and their prospective students' cybersafety issues. Braxton (2014) highlighted that raising ethical sensitivity in ICT use has a positive effect on information security awareness.

Since there is no clear guideline on increasing the pre-service teachers' information security awareness and cyberethics sensitivity level, the critical characteristics of such a course need to be explored for specific content and learners who take the course. To explore these points, design-based research methods guided this study. The first and major step of the design-based research is to specify the problem. Although the inadequacy of information security awareness and ethical sensitivity is stated as a problem, the lack of a suitable instructional tool to address these issues is the main concern of this study.

1.3. Purpose and Scope of the Study

This study aims to uncover the critical points to be considered when designing, developing and implementing a course for improving pre-service teachers' information security awareness and cyberethics sensitivity. Several strategies are focusing on information security issues. However, the attempts aiming at raising end

users' information security awareness are limited to specific warnings, such as phishing attacks or virus threats. Besides, there is a shortage of content regarding cyberethics issues for pre-service teachers.

The purpose of the study is to propose a guideline and a course to raise information security awareness and cyberethics sensitivity for pre-service teachers irrespective of their majors. In-line with this goal, firstly, a course for pre-service teachers is designed, developed and implemented to raise their information security awareness and cyberethics sensitivity by employing rapid prototyping design model. Secondly, the critical issues related to design, development, implementation as well as evaluation phase for the course are pointed out, and solutions to these issues are proposed.

1.4. Research Questions

The purpose of this study is to explore critical points on the design, development and implementation process of a course to raise the pre-service teachers' information security awareness and cyberethics sensitivity in a Faculty of Education. Therefore, the guiding research questions of the study are as follows:

1. What are the key factors encountered during the design and development of a course in an attempt to raise the pre-service teachers' information security awareness and cyberethics sensitivity?
    a. What are the content related issues?
    b. What are the learner related issues?
    c. What are the instruction related issues?
2. What are the possible influencing factors for the design, development, and implementation process of the course?
    a. What are the facilitating factors?
    b. What are the challenges and how are they handled?
3. How do pre-service teachers perceive the contribution of the course on their information security awareness and cyberethics sensitivity?

1.5. Significance of the Study

International Telecommunication Union (ITU) reported a Global Security Index in 2014, and 2017. Different indicators including legal, technical, and organizational measures and capacity building and cooperation parameters were used in this report. Turkey's global security rank was 22 out of 196 countries in 2014 (ITU, 2015). In 2017, however, after new parameters regarding professional training, educational programs about cybersecurity and cyberethics issues included in the survey, the rank slipped to 43 out of 193. This decline indicates that cybersecurity training is a requirement for all components of information related institutions, including educational settings.

Being an experienced employee in the computer center of a public university, the researcher has observed several security breaches and incidents caused by university students. There are several in-service information activities for the university staff. Only, as a subgroup of university staff, computer center employees were given different kinds of security training related to their job descriptions. These pieces of training are provided as a part acquiring ISO 27000 certification which is the international standard of information security given by The Information Standards Organization (ISO). Most of the effort aiming at raising information security awareness for the other constituents of the university (academic and administrative staff, students) is limited to sending messages and warnings in critical situations, or warning the victims when a security incident is detected. For example, in the cases of an imminent cyber threat such as a break-out of a particular virus attack, warning e-mails are sent to all constituents to be wary of the danger, update their antivirus software and not to open unknown e-mail attachments. Phishing warnings are also issued from time to time.

The researcher also observed that ethical sensitivity of the institution is mainly focused on plagiarism detection, prevention of mass downloads from subscribed e-resources such as e-journals or ethical use of online questionnaires for human-oriented research. The general netizenship principles, privacy and cybersafety issues are of much less concern.

There is a course given by Informatics Institute to students of the whole university in their first years, namely “Introduction to Information Technologies and Applications,” aiming at training digital literate students. The non-credit course covers the general topics on operating systems, office programs, and elementary computer security skills. This course is not compulsory for the students of the Faculty of Education, because their curriculum includes another similar but 3-credit course. The objectives of the course are to develop familiarity with basic concepts of computer literacy, ability to use some software such as word-processing, presentation or spreadsheets software, and making students capable of using Web 2.0 tools.

Having made these observations and taking them into consideration, it is believed that a semester-long course with online and face to face interactive instructional activities would be beneficial to be effective in imparting the cyberethics, cybersecurity and cybersafety concepts to the students. Another factor in this decision was that seminars or different methods of information transfer would not be sufficient for covering all the relevant topics. Because; the students' interest, participation and contribution to a credit course they had enrolled would be at a higher level compared to that of a seminar or a non-credit course. Furthermore, the seminars aiming at raising end users’ information security awareness does not include discussion and learner interaction.

1.6. Definitions of Terms

Cybersafety deals with the actions individuals take to minimize the dangers they could encounter when using Internet-capable technology (Pusey & Sadera, 2011).

Cybersecurity and information security are always used as synonyms, but there is a significant difference. Cybersecurity is defined as “the ability to protect or defend the use of cyberspace from cyber-attacks (NIST, 2013, p. 58).” It is about securing things that are vulnerable to ICT.

Cyberethics is the philosophic study of ethics about computers, encompassing user behavior and what computers are programmed to do, and how this affects individuals and society. For years, various governments have enacted regulations while

organizations have defined policies about cyberethics. In this study, Cyberethics is defined as the moral choices individuals make when using Internet-capable technologies and digital media (Pruitt-Mentle & Pusey, 2010). Cyberethics issues include online etiquette, copyright, freedom of speech, and ethical behaviors through the internet.

Design-Based Research (DBR) is a type of research methodology in the learning sciences. Interventions are conceptualized and then implemented iteratively in natural settings to test the ecological validity of the theory and to generate new theories and frameworks for conceptualizing learning, instruction, design processes, and educational reform. Data analysis often takes the form of retrospective, cross-iteration comparisons (Van den Akker, Gravemeijer, McKenney, & Nieveen, 2006).

Digital Citizenship is briefly defined as the norms of appropriate, responsible technology use (Ribble, 2009). It has nine elements which are the fundamental concepts of digital citizenship. They are; Digital Communication, Digital Law, Digital Access, Digital Commerce, Digital Security, Digital Rights, and Responsibilities, Digital Health and Wellness, Digital Literacy, and Digital Etiquette.

End User is defined as "An individual who uses computer applications for his/her daily work" (Whitman & Mattord, 2012, p. 585).

Ethical Sensitivity is the ability to identify a moral problem and to understand the ethical consequences of the decisions made (Tuana & Vasko, 2015).

Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction (Whitman & Mattord, 2012, p. 588).

ISO/IEC 27000 is a family of standards on information security management systems whose objective is to help organizations to keep their information assets secure (ISO, 2017).

Security Awareness is a state where users in an organization are aware of – ideally committed to – their security mission often expressed in end user security guidelines (Siponen, 2000, p. 31).

CHAPTER 2.

LITERATURE REVIEW

This section aims to summarize and synthesize the literature related to the research questions presented in the previous chapter. Firstly, information security and cyberethics training attempts in different work domains are described. Then, the conceptual definitions, commonalities of and distinctions between the terms information security, cybersecurity, cybersafety, and cyberethics are presented. Later, the literature related to information security and cyberethics training and research studies aiming at raising information security awareness and cyberethics sensitivity in educational settings has been reviewed. The scholarly attempts are introduced. Instructional frameworks about digital citizenship and C3, namely cyberethics, cybersafety, and cybersecurity are described. Finally, the findings of the need analysis of the study and course content development studies were summarized and presented.

2.1. Information Security and Cyberethics Training

The recent research studies indicate that the institutional attempts aiming at raising information security awareness generally focus on information technology employees (Burns, Roberts, Posey, Bennett, & Courtney, 2015; Mutchler, 2012), military services (Berry, Vin, & Ieee, 1996; Borges, Martins, Andrade, & dos Santos, 2015) or financial customers (Albrechtsen, 2007; Bang, Kim, & Hwang, 2008).

Information security related threats diversified year by year. In the early years of ICT technologies, major threat was virus attacks or employee oriented problems.

Intellectual property protection was also a major concern of industrial work environment (Kritzinger & Smith, 2008; Waly, Tassabehji, Kamala, & Ieee, 2012). The security measures were generally taken by system administrators (Goodhue & Straub, 1991). These measures usually are limiting authentications and employing security policies and procedures. However, these measures have no significant effect on users' security behavior (Waddell, 2013). The training programs aiming at raising employees' information security awareness level were limited to institutional settings and were not suitable for generalization to different work domains. The focus of organizational security training programs was on procedural and behavioral change. Nowadays, phishing attacks through social media (Çakır et al., 2015) and mobile applications security (Allam et al., 2014) gained more attention. The spread of mobile technologies and the ease of online access caused an increase in phishing attacks through mobile communication.

As ICT technologies penetrate deeper into the general society and the threats diversify, the need for the security awareness and cyberethics sensitivity for both the general public as well as the members of different professions has increased (Pusey & Sadera, 2011; Ryan, 2006; Woodhouse, 2007). In particular, end user training has critical value in securing the information-dense environment (Decker, 2008; San Nicolas-Rocca & Olfman, 2013). As pointed before, teachers have a crucial role in raising the future generations, so they should be well prepared to cope with the challenges brought about by these trends (Andersson & Reimers, 2012; Keengwe & Agamba, 2012).

In this section, up to this point, the early efforts of information security awareness and measures against information security related threats were presented. The role of end users' information security awareness is emphasized. Throughout this section, information security, cyberethics, cybersafety, and cybersecurity concepts from the educational perspective are introduced with related literature.

2.1.1. Information Security, Cybersecurity, Cybersafety, and Cyberethics: Overlaps and Distinctions

The term "information security" is generally regarded as the technical measure, such as network security or hardware security. The protection measures are also at the technical level, and the training attempts are at a procedural and managerial basis. On the other hand, information security threats are not only at the cybersecurity level, but the safe and ethical use of digital resources is also a primary factor for information security. Pruitt-Mentle (2000) proposed a holistic view on the secure and safe use of ICT resources and proposed a framework with the terms cybersecurity, cyberethics and cybersafety (C3). Information security and cybersecurity are regarded as synonyms and used interchangeably (Jacobson & Idziorek, 2016). On the other hand, there are some distinctions between information security and cybersecurity.

The International Standard Organization (ISO) defined Information security as:

> *"Preservation of confidentiality, integrity, and availability of information. Besides, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved (ISO, 2018)."*

With the base of this definition, information security is described as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability (CIA).

Cybersecurity, in short description, refers to the process of protection. The standards, guidelines, procedures, and security measures to maintain protection are considered as part of cybersecurity. According to the International Telecommunications Union (ITU) cybersecurity is defined as follows:

> *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and*

> *technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber-environment. The general security objectives comprise the following (i) Availability (ii) Integrity, which may include authenticity and non-repudiation, and (iii) Confidentiality (ITU, 2008, p. 2).”*

The confidentiality, integrity, and accessibility objectives have a pivotal role for both terms, and this rationale is common for both information and cybersecurity terms. On the other hand, from a protection perspective, information security seems to have a broader context compared to cybersecurity. Because information security deals not only with computer related information but also printed/hand-written information sources as well. The primary focus of cybersecurity is cyber-environment.

From the perspective of the threat, cybersecurity has a broader scope. Having secure systems is essential, but the threats in the cyber world are not limited to ICT infrastructure which is the main focus of information security. Solms and Niekerk (2013) highlighted the limitations of information security definition with the emphasis on behavioral threats through the cyber world.

For example, cyberbullying, addiction or the physical threats of overuse of the devices, information leakage by the misuse of social media are not part of the formal scope of information security. If the source of threat exists in a cyber-environment, the assets to be protected would not be limited to various sources of information; but intangible assets, such as reputation or legal rights of an individual are also in the scope of protection. In Figure 2.1, the security domains are visualized by Solms and Niekerk (2013).

Cybersafety and cybersecurity is another confusing pair of terms. As described above, cybersecurity is about protection against all kinds of threats originated through cyber-environment, such as the Internet, computer programs or mobile devices. Cybersafety, briefly, is a way of safe and responsible use of ICT resources and ensuring the safety of individuals (Pusey & Sadera, 2011).

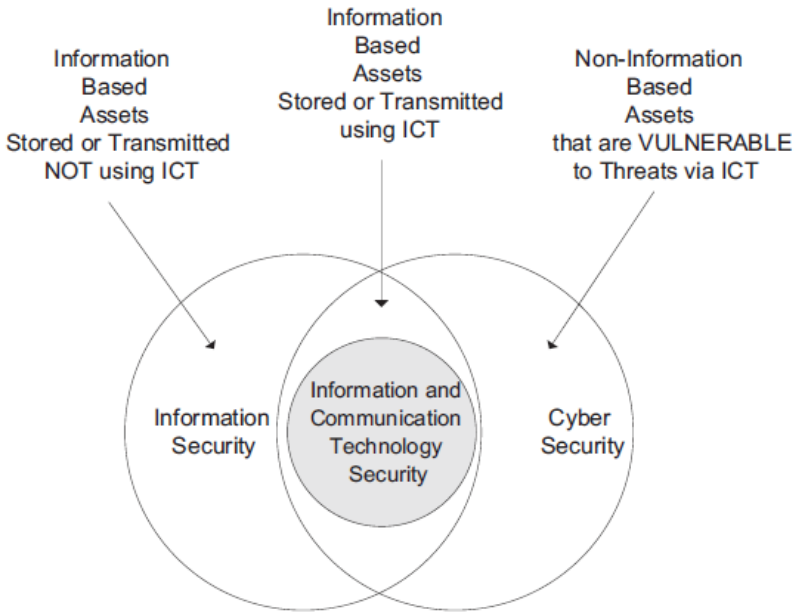


Figure 2.1. The relationship between ICT security, information, and cybersecurity.

Reprinted from "From Information Security to Cybersecurity" by R. v. Solms and J. v. Niekerk, 2013, *Computers & Security* 38, 97-102, p. 101 Copyright 2013 by Elsevier Ltd. Reprinted with permission.

In schools, safe use of ICT resources has a more critical role, because the students are vulnerable individuals for possible cyber threats such as bullying, addiction or inappropriate contents. The moral codes have an essential part in cybersafety concern. The ethical use of ICT resources also has a critical role since promoting ethical use has a significant effect on such behavioral safety threats. English Language Learners Dictionary from Merriam-Webster defined ethics as;

> *"An area of study that deals with ideas about what is good and bad behavior, a branch of philosophy dealing with what is morally right or wrong (Merriam-Webster, 2018, para. 2)."*

Cyberethics, in this case, deals with ideas about good and bad behavior through the use of ICT resources. "*Encyclopedia of Sciences and Religions"* defined cyberethics as:

> *"a branch of applied ethics that examines moral, legal, and social issues at the intersection of computer/information and communication technologies (Tavani, 2013, p. 535)."*

There is no particular overlap in definitions of cyberethics and the others while the former terms, information security-cybersecurity or cybersecurity-cybersafety pairs have overlapping use in the literature. On the other hand, some of the cybersafety issues are the results of lack of ethical sensitivity of the users (Georgia & Iliada, 2014; Irene & Libi, 2016). For this reason, cyberethics with cybersafety and cybersecurity are essential components of secure and safe use of ICT resources (Pruitt-Mentle, 2000).

2.1.2. Information Security and Cyberethics Training in Educational Setting

Information security is an important concept for teacher training. Recent studies aimed at determining the pre-service teachers' information security awareness indicate that their awareness level is not at a sufficient level (Akgun & Topal, 2015; Al-Janabi & Al-Shourbaji, 2016; Beranek, 2009). The attempts aiming at raising teachers' information security awareness are generally limited to publishing governmental issues or institutional announcements. The informative web sites are also another example of efforts on raising information security awareness (Mert et al., 2012). All these attempts are devoid of interaction and based on a passive method of information transfer.

The pre-service teacher education programs are generally based on the following four components; (i) subject matter courses; (ii) professional courses, such

as methods of teaching through different environments; (iii) courses about theoretical aspects of education; and (iv) practice course (Ben-Peretz, 1994 as cited McKenney, 2001). With the inclusion of ICT technologies, digital literacy courses and technology-enhanced instruction courses are included in pre-service teachers' education curriculum.

In Turkey; Council of Higher Education (CoHE) changed the curriculum of teaching training institutions. In the scope of the new curriculum a course aiming at raising the digital literacy of pre-service teachers was included (2018b). The objectives of the course were limited to increase the digital literacy of pre-service teachers when using computer programs for instructional purposes. In the course, the cyberethics issues are limited to copyright issues and cybersafety issues were limited to potential harms of the internet. A course covering information security and cyberethics was also suggested only to the students of Computer Education and Instructional Technology (CEIT) departments (CoHE, 2018a). The scope of that course covers the elementary issues of digital citizenship and the concepts of cyberethics, cybersafety, and cybersecurity at the introduction level.

This change in the curriculum demonstrates that CoHE attaches importance to the secure and safe use of information systems in education. Even though CoHE mandates this course as a compulsory course only for CEIT students, safe and secure use of ICT is an important issue for all subject prospective teachers (Gokmen & Akgun, 2015; Kimmons & Veletsianos; Özer & Özer, 2018; Yavanoğlu, Sağıroğlu, & Çolak, 2012).

Computers and information systems are taking a larger and larger place in our lives as well as in educational settings. Therefore, decisions are required for the right or wrong use of computers and the internet. Instruction on the ethical use of information systems and raising the sensitivity on the ethical use of digital properties and personal information are necessary (Hamiti et al., 2014; Kruger, 2003).

Cohen and Cornwell (1989), highlighted three main concerns on ethics training in information systems (IS) such as (i) wherein the curriculum should ethics would be

thought, (ii) which pedagogy could be used and finally, (iii) how the ethical issues could be explored. As the first concern, cyberethics concept might be thought as a separate section on IS curriculum. Another approach is to integrate ethical issues overall IS related courses. For example, to incorporate a code of ethics into IS course content gives the learners "a sense of right and wrong, and have a commitment to behave accordingly (p. 432)."

Kruger (2003) suggested three methods for cyberethics training of teachers.

1. *Teaching by example:* Includes ethical use of computer resources and to demonstrate the moral decisions on computer use, such as showing the copyright license, license key on the software. In an instructional setting, the demonstration of example includes in class discussion or debates.
2. *Including cyberethics into assignments:* This includes defining the terms such as copyright, intellectual property, and plagiarism or pointing out the proper methods of citing others' ideas,
3. *Seeking online cyberethics resources*: He suggests several online resources hosts by Non-Governmental Organisations (NGO) and Non-Profit Organisations (NPO).

Secure use of sources for teachers is an issue of their professional ethics since they have their students' private information (Lehto, 2015). Ethical issues in the use of ICT sources in teaching activities are not limited to right or wrong decisions in their instructional activities. In fact, with the inclusion of social network sites into our lives, teachers' ethical decision broadens from instructional facilities to their daily lives as much as they shared in the social network sites (Timm & Duven, 2008). Their posts affect their digital identity. (Ivester, 2011) The ethical decision in instructional activities includes but not limited to intellectual property issues (Klein, Moss, & Edwards, 2015), netiquette principles about their online communication with their students, or students' parents and privacy issues regarding them and their students have importance (Gallant, 2011).

There are instructional frameworks for digital citizenship or information security training in education as well. Two of them are presented in this dissertation in detail. Ribble (2006) proposed a guideline to implement digital citizenship instruction program, and Pruitt-Mentle (2000) published a framework covering the topics cyberethics, cybersafety and cybersecurity, shortly C3 framework. Several training strategies are focusing on K12 students' safe and secure ICT use. The seminar-like activities about cyberbullying, addiction, or safe use of the resources, online information pages designed particularly for K12 students, security bulletins, or technical measures which limit the web access to prevent children from inappropriate web sites are some of them. The frameworks, digital citizenship and C3, and the other attempts to raise information security awareness in K12 are presented in the following sections.

2.1.2.1. Nine Elements of Digital Citizenship

The proper use of ICT tools with a high level of security awareness and cyberethics sensitivity is one of the indicators of being a digital citizen. Ribble (2009) emphasizes that the safe and secure use of ICT tools is a part of digital citizenship. To secure and safe use of resources is not only an indicator of professional teaching but also provides a guideline for the students about appropriate and responsible ICT use. He states that "*We need not only to educate our children on the issues that are occurring with technology but provide resources for our teachers and parents as well* (p. 16)."

Table 2.1. *Nine elements of Digital Citizenship*

Respect	Educate	Protect
Digital Etiquette	Digital Communication	Digital Rights & Responsibilities
Digital Access	Digital Literacy	Digital Health & Wellness
Digital Law	Digital Commerce	Digital Security (self-protection)

Note: Reprinted from (Ribble, 2009)

Ribble (2011) identifies nine elements of digital citizenship, in three groups; (i) respect, (ii) educate, and (iii) protect. These elements are presented in Table 2.1. The digital citizenship elements in the “Respect” group represents the learners’ respect the rights of themselves and the others. The “Educate” group includes the digital citizenship elements which learners expect to educate themselves to imply those elements. The "Protect" group includes the digital citizenship elements about which learners’ protect themselves while using ICT sources.

He defined nine elements as follows:

“*1. Digital Etiquette: Electronic standards of conduct or procedure*.

2. Digital Access: Full electronic participation in society.

3. Digital Law: Electronic responsibility for actions and deeds

4. Digital Communication: Electronic exchange of information.

5. Digital Literacy: Process of teaching and learning about technology and the use of technology.

6. Digital Commerce: Electronic buying and selling of goods.

7. Digital Rights and Responsibilities: Those freedoms extended to everyone in a digital world.

8. Digital Health and Wellness: Physical well-being in a digital technology world.

9. Digital Security (self-protection): Electronic precautions to guarantee safety (p. 79).”

In the US, these elements are being taught with related examples to foster good digital citizenship. For example, “Digital Access” states equal access for all students. The school is supposed to provide access to students with special needs.

The cyberethics related scenarios and current events guide digital citizenship activities. The course designed in the scope of this research includes scenarios in the course.

2.1.2.2. C3 Framework: Cybersecurity, Cybersafety, Cyberethics

There are several ethical and safety issues in the use of ICT resources. International Society for Technology in Education (ISTE) published a report about safety issues in schools regarding the use of digital resources. In this report, Robinson (2010) summarized the possible safety threats as follows;

"*1. Inappropriate content*
2. Predators, or ensnarement
3. Misuse of mobile communication devices
4. Cyberbullying
5. Network security
6. Inappropriate network use
7. Copyright infringement
8. *Data and identity theft* (p. 10)."

Since schools are information-dense environments, information security is an important issue, but safety and ethical issues also have important roles. Developing ethical and responsible behavior on the use of ICT is not a new phenomenon in education. IT managers utilize age filters. School administrators force teachers and students to limit their use of cyber resources. These external strategies may work when utilized but do not affect a behavioral change in the individual (Pruitt-Mentle, 2000; Pusey & Sadera, 2011).

For this reason, to raise information security awareness and cyberethics sensitivity of teachers, a holistic approach on the safe, secure and ethical use of ICT resources is necessary. As a result of these requirements, an instructional program on cyberethics, cybersafety, and cybersecurity, namely C3 framework has been devised.

C3 framework is developed for both teachers' and students' safe, secure and ethical ICT use. The focus of the C3 framework is to teach basic digital netizenship principles to the students. As presented in Figure 2.2, these three concepts are not semantically separate. On the contrary, they have common issues with each other. For example, a teacher is expected to use IT resources in safe and ethical behavior. In case

of a security breach, the information assets which the teacher holds become vulnerable. In this case, not only the teacher's privacy but also the students' may be vulnerable to threats. Taking necessary measures for information security is a part of professional ethics for the teachers.

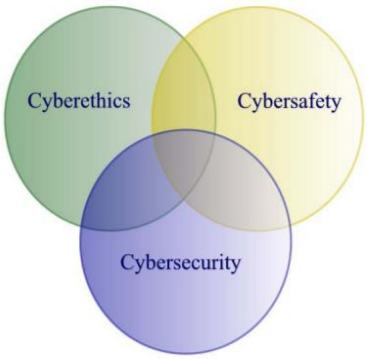


Figure 2.2. C3 Framework; Learning Areas for Policy Development

From "C3 Framework Cyberethics, Cybersafety, and Cybersecurity Promoting Responsible Use" by D. Pruitt-Mentle, page: 1 (2000). Copyright © 2009 by ETPRO; Educational Technology Policy, Research, and Outreach, Reprinted with permission

Cyberethics deals with "moral, legal, and social issues at the intersection of computer/information and communication technologies (Tavani, 2013, p. 535)." Regarding this definition, general netiquette principles, digital reputation, ethical use of public ICT sources, and code of ethics, academic integrity with ICT use, intellectual property, and free speech are some of the main concepts deals within cyberethics theme.

ISTE suggests a group of standards for educators. In-line with these suggestions, the educators are expected to create experiences for learners to the responsible use of ICT resources, to establish a learning culture to promote safe and secure ICT use, and mentor students in secure, safe, moral and legal practices with ICT tools.

C3 conceptual framework is being used in in-service training in K12 level (Kritzinger, 2015). Kritzinger (2015) suggests that training cybersecurity concepts

with short term activities influence the students for a limited time. For a permanent behavioral change, however, to integrate C3 topics into the curriculum is necessary.

Teachers feel they are low prepared for teaching C3 topics, mainly cybersecurity-related topics (Pruitt-Mentle, 2011). Pusey and Sadera (2012) highlight that, training pre-service teachers on digital citizenship is not limited to the developing knowledge of these concepts. They suggest that future teachers should be well trained to inform their prospective students about possible threats of poor digital citizenship.

2.1.2.3. Different Methods and Attempts for Information Security and Cyberethics

There are several web-based sources for K12 students. Çiftçi and Delialioğlu (2016) developed a security portal aiming at supporting students' information security related skills. The portal was an extracurricular portal and was not a part of the instructional process in schools. The portal included information about security threats, vulnerability types and protection measures, risks of SNSs on privacy. Their study concluded that the students were heavy users of SNSs and vulnerable to security threats.

Information and Communication Technologies Authority in Turkey prepared a web site, "http://www.guvenlicocuk.org.tr/," for children and teenagers. The web site included information, animations, and online games. The primary purpose of the web site was to promote secure and responsible internet use, prevention from addiction and cyberbullying.

Mert, Bülbül, and Sağıroğlu (2012) reviewed the protection and information strategies in Turkey. The review results indicate that these web sites were not sufficient to establish responsible and secure ICT use. They advocate that creating a behavioral change requires the contributions of all parts of education, including educators, school administrators, parents, and students.

Akbulut and Çuhadar (2011) conducted a study on cyberbullying with 55 pre-service teachers. The study included a 2-hour lecture explaining general information

about and necessary actions to take in case of cyberbullying. In the end, a visual demonstration of cyberbullying incidents was presented. The study concluded that the lecture has an influence on pre-service teachers and they would feel responsible for preventing a possible cyberbullying incidence in their personal lives. The designed course also has three lecture hours discussion session and online activities dedicated to cyberbullying, and it is believed that it will help improve pre-service teachers' awareness of this issue.

2.2. Literature in the Scope of Course Design and Development

The researcher of this study benefitted from a variety of sources for a wide range of topics both in the design of the course and. In the design of the course, a needs analysis study was conducted. In that phase, the semi-structured interviews with the informants and reviews from the security reports and survey studies guided the preparation of the content pool of the study. In the first part of this section, reviews from the sources are presented. The methods of selection are explained in Chapter 3 in detail. In the second part, the samples of similar courses were reviewed. The course objectives, covered topics, and evaluation methods were compiled and listed. Finally, in the third part, the literature reviewed in course implementation phases are presented.

2.2.1. Literature Guiding the Needs Analysis

The researcher reviewed several survey studies on information security and cyberethics, which are conducted with end users. The selection of the studies was depended on the following criteria; (i) focus of concern would be the information security or cyberethics issues in the use of ICT and (ii) the participants of the study were the students either in a K12 school setting or at the university level. In some cases, the studies carried on with end users who were not members of an educational domain but not at IS professional level were also considered. The references of the reviewed surveys are listed in Appendix A.

Kaya and Kaya (2014) evaluated the pre-service teachers' *digital citizenship* perception of pre-service teachers. In their qualitative study, they interviewed ten pre-

service teachers' digital citizenship perception. According to the result of the study, all of the pre-service teachers participated in the survey said that they used the internet for connecting other people through *social network sites* (SNS). The second most frequent reason for using the internet was to do homework and research. The participants feel safe when *online shopping* from the advertised companies. Kaya and Kaya resulted that the interviewees (8 of 10) have a false assumption of advertised companies are secure. Only three participants stated that they take care of the security level of an online shopping site.

In the context of *information security*, the threats about mobile devices draw attention. Poll (2015) reported a dramatic rise in the use of mobile devices in schools. He surveyed with a total of 2274 students including 507 elementary schools (4^{th} – 5^{th} grade) students, 760 middle schools (6^{th} – 8^{th} grade) students, and 1007 high school (9^{th} – 12^{th} grade) students in the United States. He underlined that more than half of the elementary (53%) and middle school (66%) students and a vast majority of high school students (82%) regularly use mobile phones.

In Turkey, the Turkish Statistical Institute (TUIK) reported that the use of mobile devices out of the overall population in Turkey is 96% and internet subscription was 85% in 2017. The internet subscription was 30% in 2012, whereas the mobile phone subscription was 87% (TUIK, 2018). With the spread of mobile internet in Turkey, Internet subscription has been increased dramatically. The leading reasons for Internet usage were reported as "Participating in social networks (creating a user profile, posting messages or other contributions)" with 84.1%.

Allam and his colleagues (2014) highlighted *mobile device security* issues and underlined that the users are unaware of the basic security procedures of mobile devices. Although the scope of the study was business employees, the case is not different among the students and the teachers since the end users are selected from non-IS department employees. Riola (2014), surveyed the college students' *mobile security* behaviors in his quantitative study with 573 respondents. He concluded that students' security awareness of mobile technologies is inadequate. The college

students were vulnerable to *malicious applications* or any loss of information in case of device theft.

The rise in the use of smartphones and mobile internet increased communication-related concerns. *Teacher-student communication* and *teacher-parent communication* were two critical privacy and ethical issues in an educational context (Thompson, Mazer, & Flood Grady, 2015). Ease of access to the internet came with the threat of *malicious profiles*, and *fraudulent content*.

Hanus (2014) conducted a *phishing* experiment to identify click rates of different types of phishing e-mails. The target population of the study was limited to the employees of a municipal organization. In the experiment, he constructed two types of phishing e-mails; one of them was labeled as regular phishing e-mail, which is similar to commercial spam e-mails. Their response rate is around 2.7%, and it was in line with the click rates of similar scam e-mails. Another type of phishing e-mail was spear phishing e-mail, and generally, it is regarded as an example of social engineering. The e-mail seemed to be an official e-mail, sent by the IT team of the institution. There were little details to notice the phishing trap. The response rate was 16%. The increase in the click rate indicated that explaining the types and characteristics of phishing e-mails and web sites in the course was very critical.

Excessive use of computers or mobile devices, or in other words computer *addiction* is another concern of the studies. Addiction has different subtopics. Nalwa and Anand (2003) surveyed internet addiction with 100 randomly selected students in public schools. They concluded that the students feel life would be boring without the internet. The respondents also state that they have failed to control the time spent during online activities. Internet addiction commonly rises through online activities, such as social networking sites (SNS) or online games. Kuss and Griffiths (2011) studied social networking addiction in different studies. They concluded that younger social network users were more inclined to be addicted compared to elder ones (Kuss & Griffiths, 2011). Later, they published ten critical points for internet addiction research, which is also beneficial for the course. Their synthesis of findings is;

"1. Social network and social media users are not the same;

2. *Social networking is eclectic;*
3. *Social networking is a way of being;*
4. *Individuals can become addicted to using social networking sites;*
5. *Facebook addiction is only one example of SNS addiction;*
6. *Fear of missing out (FOMO) may be part of SNS addiction;*
7. *Smartphone addiction may be part of SNS addiction;*
8. *Nomophobia may be part of SNS addiction;*
9. *There are sociodemographic differences in SNS addiction; and*
10. *There are methodological problems with research to date (p. 2)."*

The security and safety issues in the use of social network were not limited to addiction. Privacy issues of social media is also another point of concern. Yıldırım and Varol (2013) surveyed 306 participants, 211 were students, and 95 of them were instructors or faculty members in two universities in Turkey. They found that the participants have a low-level awareness on privacy issues of SNSs. Majority of the participants share their private information correctly (78%), The SNS users who participated in this study share their photographs (30%), day of birth (25%) or e-mails (30%). More than one-third of the participants (38%) check security settings once a month. A surprising result they found out is that 66% of the participants said that the information shared in these SNSs may be used for malicious purposes. Briefly, Yıldırım and Varol concluded that the university students' information security awareness is lower than required. Although the majority of the users met some of the major SNS threats such as fake profiles, malicious links, or harassing contents, this situation does not stop them from sharing their private information.

The dense use of social media brings another security threat, which is *cyberbullying*. Kowalski and Limber (2007) surveyed 3767 middle school students and found that more than 10% of the students have been bullied at least once in recent few months. The most common method of cyberbullying was instant messaging, chat rooms and e-mail. They concluded that school administrations should take necessary action, educate teachers and students about the effects of cyberbullying and

appropriate use of ICT resources. The situation in Turkey is similar to that of in the US. Sezer, Yilmaz, and Yilmaz (2015) surveyed 184 teachers in different provinces and underlined the requirement of action against cyberbullying. They suggested training teachers about identifying such cases about cyberbullying. Another suggestion was raising students' awareness about the effects of cyberbullying.

Çakır and his colleagues (2015) surveyed 909 pre-service teachers about their security awareness on social networking sites. The survey indicated that pre-service teachers were aware of password security issues. They generally are aware of the information disclosure risk of social network sites. On the other hand, according to the results of the survey, they do not read the acceptable use policy statements.

Academic dishonesty has been an important issue in education far before the internet era (Cole & McCabe, 1996; Maramark & Maline, 1993) Declaring honor code is an effective way of building academic integrity (Kidwell, 2001; McCabe, Trevino, & Butterfield, 1999). The penetration of the computers and ease of access to homework solutions increased digital cheating. However, cheating and plagiarism (Ma, Wan, & Lu, 2008), specifically bilingual plagiarism (McNaught & Kennedy, 2009) remains as a dishonesty case.

Briefly, end users' attitudes when using the ICT sources were investigated. The sharp increase in the use of mobile devices increased both privacy and hardware security risks. Social networking sites are other critical threat to privacy. Malicious profiles and fraudulent contents are threats to users' privacy. The findings of survey research and contribution to course contents are listed in Table 2.2.

Table 2.2. *The Findings of Survey Studies*

Survey	Major Finding	Topic
Poll (2015)	Increase in use of Mobiles at the K12 level	Mobile security
TUIK (2018)	Increase in use of mobile devices with the inclusion of the internet	Mobile security
	Most frequent use is on Social Network Sites (SNS)	SNS Privacy
Allam et al. (2014)	End users fail to recognize malicious applications on their mobile devices	Mobile security
Riola (2014),	Loss of the information in case of theft	Mobile security Hardware Security
Hanus (2014)	The style of phishing affects deception rate.	Phishing
Nalwa and Anand (2003)	The students fail to control the time spent on Internet activities	Internet Addiction SNS Addiction
Kuss and Griffiths (2011)	Younger SNS users were more inclined to be addicted compared to older users	Game addiction SNS Addiction
Thompson, Mazer, and Grady, (2015)	Two major privacy issues in the educational context are teacher-student and teacher-parent interaction	SNS Privacy
Yıldırım and Varol (2013)	Majority of the participants share their private information."	Oversharing Privacy
	The pre-service teachers have no idea of identifying fake profile	Fraudulent content Fake profile
Kowalski and Limber (2007)	A training to prevent cyberbullying is needed	Cyberbullying
Sezer, Yilmaz, and Yilmaz (2015)	School administrations should take action to prevent cyberbullying	
Çakır et al. (2015)	Secure password strategies were not known at the adequate level	Password security
Cole and McCabe, (1996) Maramark and Maline, (1993)	Although cheating is a pre-Internet phenomenon, the internet makes it easier	Academic dishonesty
Kidwell, 2001	Honor code has a positive effect on eliminating academic dishonesty incidents	Honor Code
Ma, Wan, & Lu, (2008),	Students' cheating habits results cheating sites to increase.	Digital Cheating
Carmel & David, (2009)	The verbatim translation is a less known type of plagiarism.	Bilingual plagiarism

2.2.2. Sources Guiding the Development

In the development phase, the courses focusing on cyberethics, cybersafety or cybersecurity were reviewed. The courses and the covered topics were presented in Table 2.3. There were no common topics which all four courses have covered. The first course was an 8-week course and focused on the business case of cyberethics and intellectual property. The second course was introducing the privacy issues in SNSs at the introduction level. The third course was a 14-week online graduate course and entirely focused on cybersecurity issues. The fourth one was a 6-week graduate course and focused only on ethical uses of ICT tools.

Table 2.3. *Review of the selected courses on C3*

	Topics Covered			Evaluation Methods			
	CE	CSf	CSec	Lab activity	Forum	Take home	Participation
Course 1	*	*			*	*	*
Course 2	*	*			*		*
Course 3			*	*			
Course 4	*						

CE: Cyberethics, CSf: Cybersafety, CSec: Cybersecurity

Course 1: Cyberethics: Privacy and Intellectual Property[1]

Course 2: Cyberethics for Educators by Pruitt-Mentle [2]

Course 3: ITEC 545: Cybersecurity Education at Radford University [3]

Course 4: Cyberethics for Educators at University of Phoenix [4]

The second course was covering cybersafety and cyberethics issues at the introduction level. However, cybersecurity issues were poorly covered. The researcher

[1] APU. (2018). ISSC631 - Cyber Ethics: Privacy and Intellectual Property, from https://www.apus.edu/schedule-classes/schedule/course/issc631

[2] Phoenix, U. o. (2017). Cyberethics For Educators, retreived from https://www.phoenix.edu/courses/edu538.html

[3] Pruitt-Mentle, D. (2002). Cyberethics for Educators: Ethical and Legal Implications for Classroom Technology, retreived from http://www.edtechpolicy.org/CourseInfo/cyberethics.pdf

[4] University, R. (2017). ITEC 545: Cyber Security Education, retreived from https://www.radford.edu/content/csat/home/itec/graduate-curriculum/itec545.html

combined these topics for the development of the course as the pre-implementation phase.

Both forth and the second courses highlighted the cyberethics related misconducts, such as digital cheating, cyberbullying, free speech or digital equity. Acceptable use policy, copyright issues were also other common issues which were covered as cyberethics topics.

The evaluation methods were focused on online or in-class participation. In particular, ethics training depends on dilemmas and identifying ethical issues. For this reason, either in-class discussions or online discussion forums have an important effect on learning and comprehending the topics. For this reason, participation is included in the grading policy of the course.

2.2.3. Literature Guiding the Implementations

The researcher used several resources while preparing the course contents. The online dictionaries, reference books, security reports, constitutional acts, legislative regulations, circulars, guideline pages of the universities, and online resources managed by NGOs and NPOs were the main resources of course implementation phases.

Defining a topic is a critical issue. The researcher generally used the dictionaries of Merriam-Webster and Oxford. The technical definitions, such as Information security topics, were provided by different sources such as "*Information security terms: glossary with acronyms and abbreviations* (Cox, Ellis, Kissel, & Kent, 2012)." The terms of information security were defined from sources of ISO 27000 series (ISO, 2009, 2017, 2018).

The course provided guidelines such as "*how to prevent from phishing* (Phishing.org, 2018)," "*how to secure online identity* (Cherry, 2014)", "*what can be done in case of cyberbullying* (Eaton, 2017)" or "*how to deal with cyber addiction* (Grabianowsky, 2007)."

2.3. Summary of the Literature Review

The secure and ethical use of ICT resources gained attention in the last decades. With the penetration of mobile devices and wireless internet into our lives, the threats were diversified exponentially. At the beginning of this literature survey, the literature relating to the early attempts to raise awareness on these issues and the shift from educating IT professionals to end users is pointed out. The survey went on to clarify the potentially confusing terms of *information security*, *cybersecurity*, *cybersafety*, and *cyberethics* by referencing the relevant literature. In educational settings, the students are more vulnerable towards possible threats such as cyberbullying or identity theft. Therefore special attention should be directed to educational settings, the education of pre-service teachers being an important concern.

There are several attempts aiming at raising the children's information security awareness. Since they are digital natives, (Prensky, 2001), they are familiar with ICT resources. However, their security awareness and ethical sensitivity are not at the required level (Çubukcu & Bayzan, 2013). The conceptual frameworks such as digital citizenship and C3 were proposed to address the interrelated issues of cybersecurity, cybersafety, and cyberethics which were discussed in the subsequent parts of the literature survey. Ribble (2009) defined digital citizenship and identified nine elements of digital citizenship. Pruitt-Mentle (2000) highlighted that a holistic approach on the safe, secure and ethical use of ICT resources. They both advocate that student participation in instructional activities is required. There are several training attempts for particular topics. Each study highlights that an improvement in the teacher training curriculum to include C3 related issues is necessary.

Having seen the efforts to provide education on information security awareness and cyberethics sensitivity, the last part of the literature survey is devoted to surveying the literature which would support the research undertaken, namely needs analysis, course development, and lecture implementations. The overall result of the literature survey points out the necessity of developing a full course replete with some additional topics such as privacy and ethical issues in SNSs, cyber addiction, protection in information assets, ethical aspects of intellectual property, and hate speech.

CHAPTER 3.

THE RESEARCH METHOD

In this chapter, a detailed description of the research method is presented. First, the research questions are stated. Then, the study is described with the explanation and justification of design-based research. The Informants and the participants of the study are introduced. Design of the research environment is described. Data collection instruments and data analysis procedures are explained. After the description of the research procedure of the study, the researcher's role is given. Finally, issues of trustworthiness, limitations of the study, and ethical considerations are addressed.

3.1. Research Questions

The major objective of this study is to identify the critical points about the design, development and implementation process of a course in order to increase the information security awareness and cyberethics sensitivity of teacher candidates. For this reason, the guiding research questions of the research are as follows:

1. What are the key factors encountered during the design and development of a course in an attempt to raise the pre-service teachers' information security awareness and cyberethics sensitivity?
    a. What are the content related issues?
    b. What are the learner related issues?
    c. What are the instruction related issues?

2. What are the possible influencing factors for the design, development, and implementation process of the course?
    a. What are the facilitating factors?
    b. What are the challenges and how are they handled?
3. How do pre-service teachers perceive the contribution of the course on their information security awareness and cyberethics sensitivity?

3.2. Design of the Study – Design-Based Research

In order to identify the critical issues on course design, development and implementation, this study employs Design-Based Research (DBR) as an approach to describe the steps and results of a course development process. Design-based research is labeled in different ways in the literature. It was first proposed in the early 90s by Allan Collins (1990) and Ann Brown (1992) with the label of "design experiments." The major distinction was that the researcher took an active role in the learning and teaching process (Wang & Hannafin, 2005). Later, van den Akker (1999) proposed research principles with the label of "Developmental research." The most common names are; design experiments (Brown, 1992; Collins, 1990), design research (Oh & Reeves, 2010), design-based research, developmental research (Richey, 1994; Van den Akker, 1999).

Design-based research can briefly be described as the synthesis of design and development of solutions to practical problems in learning environments and reporting the reusable design principles (Herrington, McKenney, Reeves, & Oliver, 2007). Bereiter (2002) emphasizes the innovation producing and sustaining the developmental nature of design research:

> *"The research that produces innovations and sustains their development has come to be called 'design research.' It is any kind of research that produces findings that are fed back into further cycles of innovative design (p. 329)."*

Collins, Joseph, and Bielaczyc (2004) describe design-based research as:

> *"Design experiments were developed as a way to carry out formative research to test and refine educational design-based on theoretical principles derived from prior research. This approach of progressive refinement in design involves putting the first version of a design into the world to see how it works. (p. 18)."*

Wang and Hannafin (2005), also underlined the similarities and nuances between the terms "*design experience*," "*design research*," "*development research*" or "*developmental research*" and highlighted that primary objectives and methods were similar. They defined and highlighted the most common and major specifications in their definition of design-based research as follows:

> *"... a systematic but flexible methodology aimed to improve educational practices through iterative analysis, design, development, and implementation, based on collaboration among researchers and practitioners in real-world settings, and leading to contextually-sensitive design principles and theories (p. 6)."*

Briefly, most of the definitions highlight the progressive and flexible nature of the research approach. The research aims to focus on real-life problems and innovative treatment of the problem. Besides, to derive and report design principles when the research is finalized, is suggested.

The Design-Based Research Collective (2003), suggested five significant characteristics of good design-based research.

> *"1. The central goals of designing learning environments and developing theories or 'proto-theories' of learning are intertwined.*
>
> *2. Development and research take place through continuous cycles of design, enactment, analysis, and redesign (Cobb, 2001; Collins, 1992).*
>
> *3. Research on designs must lead to sharable theories that help communicate relevant implications to practitioners and other educational designers (cf. Brophy, 2002).*

4. Research must account for how designs function in authentic settings. It must not only document success or failure but also focus on interactions that refine our understanding of the learning issues involved.

5. The development of such accounts relies on methods that can document and connect processes of enactment to outcomes of interest (p. 5).”

Since design-based research does not follow traditional research methods, such as a classical experimental design, or formal definitions of scientific methods, it is sometimes regarded as non-scientific by traditional experimental scholars. Desforges (2000) called design experiments as “neither designed, nor experiments” and suggested that design experiments could have been linked to a scientific experiment. Easterday, Rees Lewis, and Gerber (2014) also emphasized the common problems in the application of design-based research. They addressed the uncertainty problems which are (i) uncertainty of the phases of the DBR process, (ii) Uncertainty about how DBR differs from other forms of research, (iii) lack of clear distinction between the concepts design and design research, and (iv) the characteristics of DBR that make it effective for answering certain types of questions. They suggested solutions with a clear definition of DBR. They advocated that the phases should be defined clearly. Well defining the phases allows the further steps to be easier. They highlighted the differences between DBR and other research methods as “*DBR designs a product while using other methodologies as nested processes (sub-phases) of design (p. 322).*” The distinction between design and design research is that DBR does not only designs an intervention for a problem, but with its iterative stages method, and collaboration with practitioners, DBR produces theories or general design principles. They underlined the gain of DBR by organizing the appropriately nested scientific process at a given stage of development.

Despite the controversy regarding DBR, there are sufficiently many studies in the literature. For example, when exploring the characteristics of a computer-supported curriculum (McKenney, 2001), or clarifying the design issues on a blended learning environment (Gedik, 2010) design-based research is chosen. Similarly investigating the critical design and development issues for educational robotics

training camps (Üçgül, 2012) or an electronic performance support system (EPSS) of a crime scene investigation unit (Yakın, 2012) are similar examples which are guided by design-based research methodology. Suitability of this approach for this dissertation study is further explained in the next sub-section.

3.2.1. Justification of Design-Based Research

The primary motivation of DBR is to explore unclear points of design, development or implementation phase. For vague settings or a newly implemented course, there are several issues to be considered. The content, construct or learner related items are required to be explored.

Kelly (2013) states that DBR is an appropriate research method when;

> *"1. The initial state of the study is unknown or unclear;*
> *2. Goal state(s) are unknown or are unclear.*
> *3. Operators to move from initial states to goal states are unknown or how to apply the operators is unclear (p. 138)."*

The objective of this study is to explore major issues in the design, development, and implementation of a course aiming at raising pre-service teacher's information security awareness and cyberethics sensitivity. In line with this purpose, a course is designed in three phases. In the pre-implementation phase, the analysis of the problem was clarified, and the content pool was formed. Later, in two iterative implementations, the course was broadly finalized. Since there is no clear guideline or a source for such a course, the course and course contents are designed and developed throughout the study.

The key issues during the design and development of such a course are explored throughout the study. Particularly, the content pool and the course outline are to be discovered in the pre-implementation phase of the study. Learner characteristics and their prior knowledge are unclear. As a result, instructional strategies to be used in the course are to be determined during the implementations.

MoNE and CoHE recognize the importance of these issues. In other words, actions these two government offices are taking action in line with these concerns.

Furthermore, design-based research is a viable approach in the design and development of such a course. Especially the instructional design method, rapid prototyping, is conducive to the development of such a course since it can easily accommodate the changing circumstances regarding threats and ethical issues. Hence as pointed out in Chapter 1, undertaking such an effort is believed to be an original, timely contribution to the field.

The principal goal of the course is to raise information security awareness and cyberethics sensitivity, but as was stated in the third research question of the study, how the course would affect the pre-service teachers' information security awareness and cyberethics sensitivity is unclear, and to be explored throughout the study. As a result of these vague settings, DBR is an appropriate research method.

3.2.2. Design of the Study

The design process in an educational environment aims to develop research-based solutions for complex problems in education. Independent of the purpose, the research process always contains systematic educational design processes, as presented in Figure 3.1.

The primary concern of this study is to explore essential points on developing and designing process of a course to raise the pre-service teachers' information security awareness and cyberethics sensitivity in a faculty of education. Design-Based Research (DBR) approach with qualitative methods will be utilized to answer these questions. The cyclic processes of Analysis, Design, Evaluation, and Revision activities are repeated until the planned intervention of the prototype reaches its ideal form. The most generic illustration of the design process is presented by Reeves (2006) as shown in Figure 3.2.

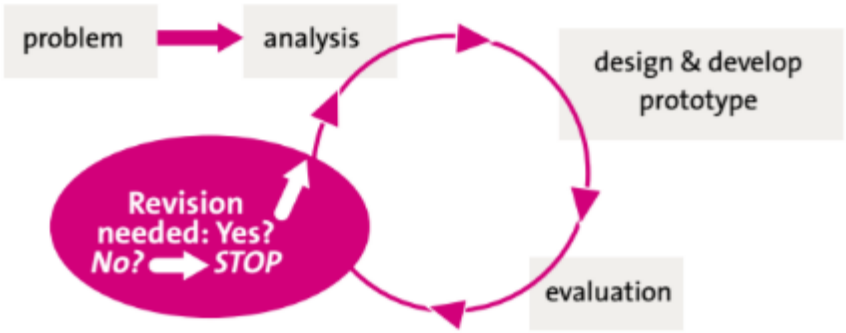


Figure 3.1. Design-based research approaches in educational technology research

Source: Adapted from Educational design research. In N. N. Tjeerd Plomp (Ed.), Educational design research. Enschede: Netherlands Institute for Curriculum Development (SLO), (Van den Akker, Bannan, Kelly, Nieveen, & Plomp, 2013, p. 17).

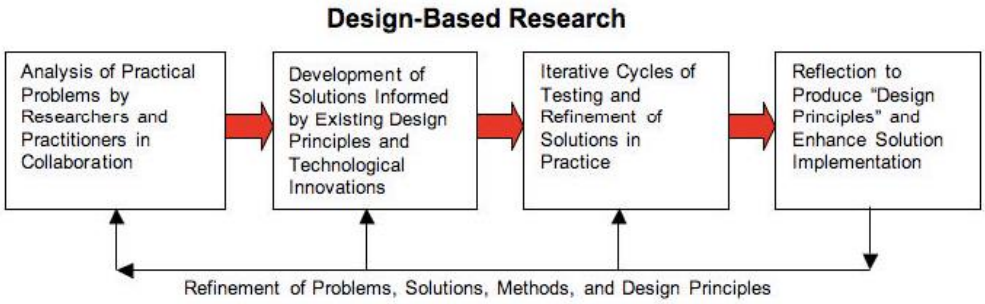


Figure 3.2. Design-based research approaches in educational technology research (Reeves, 2006).

Source: Reeves, T. C. (2006). Design research from the technology perspective. In J. V. Akker, K. Gravemeijer, S. McKenney, & N. Nieveen (Eds.), Educational design research (pp. 86-109). London: Routledge. With permission from Reeves.

At the beginning of the study, the parts of the research which are, analysis, development of a solution, iterative implementations, and finally reflection to produce design principles should be mapped according to the research requirements (Herrington et al., 2007). At the *analysis phase*, the researcher investigated the problem in detail. The *development phase* includes the design process of the course. At the *iterative implementation phase*, which refers to iterative cycles, demonstrated in Figure 3.2, the researcher conducted iteratively two implementation phases. The *reflection phase* is guided and guided by the two iterations of the implementations.

3.3. Instructional Design Model – Rapid Prototyping

Educational technology research has yielded various instructional design models over many years. ADDIE (Analyze, Design, Development, Implementation, and Evaluation), SAM (Successive Approximation Model), Rapid Prototyping (RP), Gradual Release and similar instructional design models offer frameworks to course design and development. Instructional design focuses on two basic principles; (i) a system design model for the instructional development model, and (ii) theories of high-quality instruction (Reigeluth, 1983).

Each model divides the instructional design and development process into smaller parts, but almost all models have a similar sort of analysis, development, and evaluation. Their approach to these stages may vary. When choosing the appropriate instructional design model, it is necessary to consider the content to be taught and the conditions of the course design team. Design processes generally have similar main steps: Analyzing the requirements and objectives, design of the artifact, and evaluate the results (Kruse, 2004). Instructional design is a systematic approach to the achievement of learning objectives and improving the course. Botturi, Cantoni, Lepori, and Tardini (2008) describe instructional design models as a linear step by step processes.

It is a repetitive process that continues with implementation and evaluation processes and then improves according to the evaluation findings (Daugherty, Teng, & Cornachione, 2007). Traditional instructional design approaches have been criticized in terms of their rigidity (Wedman, 1992, cited at Daugherty et al., 2007) and inflexibility (Davenport, 2006 cited at Daugherty et al., 2007). Another critical weakness of the classical linear instructional design model is that they depend on two major premises, which are; (i) the assumption of quality information, and (ii) the assumption of expertise (Boulet, 2009).

Rapid Prototyping (RP) has been proposed as a remedy to these critics by its proponents (Boulet, 2009). Tripp and Bichelmeyer (1990) suggested that this method could be considered in the instructional design process. Reiser (2001) highlighted the high interest in rapid prototyping method. Rapid prototyping is a strategy of

developing an instructional material or environment in less time compared to classical instructional design methods (Gustafson & Branch, 1997; Jones & Richey, 2000). RP aims to reduce the time and cost of the traditional ISD approach while increasing flexibility and learner engagement. In a design process, early development of a small-scale prototype is used to test out certain critical features of the design. With each iteration of prototyping, the artifact reaches its final state. RP also relies on a recursive, overlapping approach to design, rather than a linear approach through the ADDIE stages (Camm, 2012).

The significant advantage of rapid prototyping is that it makes it possible to reach a final product in a shorter time with the iterative process. The iterations are based on the interaction between users and designers. The success of a rapid prototyping method lays on the communication between the users and the designer (Aposto, 2016; Boulet, 2009). With a dynamic interaction, a designer can quickly develop the course according to the needs.

There are different workflows proposed for rapid prototyping. The events of one of the instructional design models as rapid prototyping are presented in Figure 3.3. This model is adapted from the waterfall model. The meaning of the overlapping boxes is that the various processes do not occur linearly. The iterations occur between the construction and utilization of the prototypes. The steps of Rapid Prototyping in instruction are similar to the ADDIE model, which propose to Analyze, Design, Development, Implementation, and Evaluation. The analyses step in ADDIE stands for “Needs assessment,” and constructing prototype may refer to the design and development process (Boulet, 2009; Tripp & Bichelmeyer, 1990).

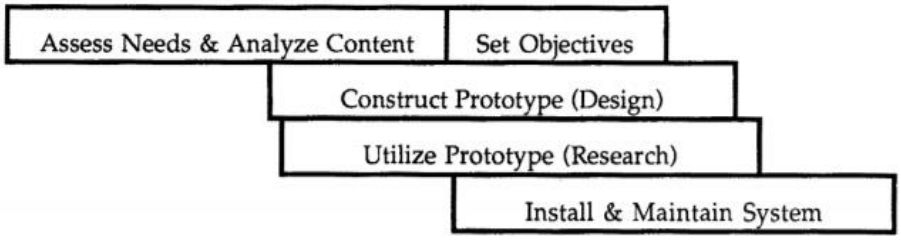


Figure 3.3. Rapid prototyping model

From "Rapid prototyping: An alternative instructional design strategy" by S. Tripp and B. Bichelmeyer (1990) *Educational Technology Research and Development*, 38(1), 31-44, p. 35, © 2018 Springer. Reprinted with permission.

Another workflow proposed for rapid prototyping is presented in Figure 3.4. The iterations occur within the prototypes and the implementations. With its non-linear approach, this workflow provides more flexibility as in the early stage of the course design. By realizing the necessary arrangements at an earlier stage, it eliminates time-consuming revisions. The design requirements are fulfilled in the process of using the product, not at the end of the project stages. In this way development time and costs are reduced. In a course design prepared by RP, students and field experts are in constant contact with the course designers. The course is presented as a prototype in the first phase, and the product development process is supported by the students and the field expert. The product improvement process is in the form of a loop. Each cycle starts at an improved stage in light of previous feedback (Camm, 2012).

The instructional design model of the study is rapid prototyping. At very early stages of planning, following the needs analysis phase, the constructed content pool exhibits major topics of the "course to be developed." In the first implementation of the course, the syllabus was redesigned according to the feedback of the enrolled students.

This prototype is explored and tested to get a better handle on the requirements of the further weeks. This process is called rapid prototyping. Its advantage is that it allows for the tryout of key concepts at early stages when costs are low, and changes are more easily made.

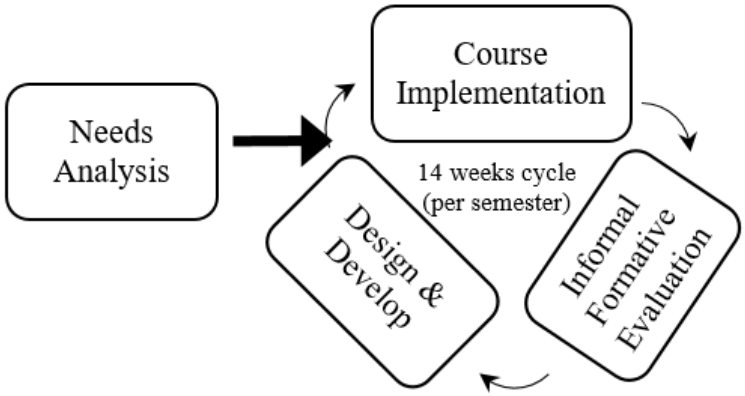


Figure 3.4. Iterations of Rapid Prototyping with cyclic workflow (Camm, 2012)

Adapted from "Instructional Design and Rapid Prototyping" by B. Camm (2012) eLearning Blog, http://www.elearninglearning.com/?query=Rapid%20prototyping&open-article-id=1374600 © 2018 2018 Dashe & Thomson.

3.4. Research Procedure of the Study

For the *analyses* and *pre-implementation* phases of the study, the researcher conducted several semi-structured interviews with SOME (Turkish abbreviation of the intervention team for cyber incidents), instructors in the department of educational sciences. The primary objective of these interviews was to identify the essential needs of pre-service teachers regarding information security and cyberethics. As a result, the content requirements of a course are explored. Explored problems found out in this stage are presented in Section 4.1.1.

The gathered information was used to generate a content pool in the first step. The contents in the pool were arranged as *a content sequence* and were presented to SOME, department chairs, and ethics specialists. Their feedback about the content sequence guided the development process and iteration cycles of the instructional tool.

At the *first implementation* phase of the study, initially, the course was designed according to the findings of the pre-implementation phase. The weekly lectures were designed with rapid prototyping strategies. The course program and the lecture presentations were also designed according to the syllabus organized with

obtained information at the pre-implementation phase. The interaction activities and course contents were developed for each week in the direction of the program.

During the *first implementation*, the students' in-class activities, feedback, participation behaviors, and exam results were observed. The course programs and the activities were designed according to the reflections obtained from the students. In the *second implementation*, the course syllabus and the subtopics were redesigned according to the findings obtained from the first implementation phase. Not only was the order of the course contents, but also the course materials provided to the students changed and improved. The primary rationale of this change was to increase the students' participation.

In the implementations, different data collection tools were utilized. Designer reflections, including the critical issues about weekly lecture preparation, and field notes, taken during the lecturing periods, guided the iterative process. Learner reflection notes obtained from semi-structured interviews with students were utilized in this stage. According to the evaluation of each implementation, successive implementations were developed. The phases according to the steps and position of the research study is presented in Table 3.1.

To summarize; in the scope of design-based research, initially, the researcher conducted a needs analysis. The expert interviews, with information security experts in the computer center, the instructors in the department of philosophy, faculty of medicine and faculty of education contributed to the study. Besides, a review of cybersecurity reports and the survey studies were conducted. As a result, a draft content pool emerged.

Later, in the development phase, follow-up interviews were conducted with the experts met in the pre-implementation phase. Furthermore, the researcher also interviewed with three university students to ask their general preference from a course.

Table 3.1. *Description of the phases*

Research Phase	Research Procedure	Research Instruments	The Outcome of the Phase
Pre-Implementation Phase: • Needs analysis and • Development of the Course	• Review of the literature of cyberethics and information security • Interviews with experts	• Expert opinion • Field notes	• The content pool • A draft outline of the course for the first implementation
The First Implementation Design and Development of the First implementation of Course	• Design of the course • Development of the course content and interaction and evaluation tools • Construction of the LMS environment of the course.	• Field notes, • Designer reflection, • Learner reflections	• Guidelines for the preparation of the second implementation • Revision in the content sequence
The Second Implementation Design and development of the Second (improved) implementation	• Development of the interaction and evaluation tools in LMS of the course • Construction of the lecture notes documents • Structured interaction tools in the forum page of the course	• Field Notes, • Designer reflection, • Learner reflections	• Guidelines for the preparation of the further implementations • Content sequence finalized

In the third phase of the study, the iterative implementations were done. With the results of the experiences had in the first implementation, the second implementation was designed and developed. Lastly, the overall reflections were found out, and are presented in the fifth chapter.

3.5. Informants and Participants of the Study

In this study different types of informants, such as IT security experts, faculty members, the students contributed at various stages of the research. Informants are described according to their contribution.

In the *analysis phase* the subject experts, with whom the semi-structured interviews were conducted, were selected according to their expertise. Three faculty members at the Department of Computer Education and Instructional Technology (CEIT), three information security experts in the Computer Center, a faculty member having expertise on ethics from the Department of Philosophy and computer coordinators of the Faculty of Education were the informants of the *analysis phase* of the study. They contributed to constituting the content pool.

In the *development phase*, the information security experts and the faculty members of CEIT and Department of Philosophy, who took part in the analysis phase of the study contributed to design of the course and the content sequence, particularly at the pre-implementation phase. Furthermore, two faculty members from the Department of Educational Sciences (EDS) and one faculty member from the Faculty of Medicine, who has expertise in deontology, were joined to the study as the informants. The members from EDS contributed to designing the outline of the course. The member of the Faculty of Medicine was consulted about the ethical context of the course in the following implementations. These informants were also advised about the lecture design and change in the content sequence between two implementations.

In the *iterative implementation phases*, two iterations were conducted. The pre-implementation phase was related to the core design of the course. For the first and the second implementations, the students who registered to the course were the participants of the study. At the beginning of each semester, in the first meeting session, the prospective course students were informed about the nature of the study,

and they are also told that the course was in the development phase. Telling the students about this issue is a part of the ethics code of the research study.

The contribution of the students to the study was not limited to being a registered student. As the *reflection phase;* for each semester, the researcher conducted semi-structured interviews with voluntary students. Those who accepted to participate in the interviews were the participants of the reflection phase of the study. In summary, 15 out of 40 students from the first implementation and 8 out of 21 students from the second implementation were the participants of the interviews. The information about the duration of the interviews is presented in Table 3.2.

Table 3.2. *Duration of the Interviews*

Code of the Interviewee	Duration of the Interview
M101	0:17:16
M102	0:13:00
M103	0:14:13
M104	0:16:19
M105	0:20:29
M106	0:08:28
M107	0:12:15
M108	0:11:20
M109	0:09:05
M110	0:10:51
M111	0:06:40
M112	0:11:02
M113	0:07:33
M114	0:05:18
M115	0:19:49
M201	0:18:33
M202	0:15:11
M203	0:13:15
M204	0:20:14
M205	0:15:18
M206	0:25:24
M207	0:22:09
M208	0:16:47

The information about departments, gender, and grades of the interviewees are presented in Table 3.3.

Table 3.3. *Department, Gender and Grade Information about the Interviewees*

Department	N
CEIT	22
EME	12
FLE	4
Gender	N
F	15
M	25
Grade	N
AA	17
BA	3
BB	2
CB	1

3.6. Data Collection Instruments

Design-based research with a qualitative approach is carried out in this study. In this approach, the following instruments are utilized.

- ***Expert interviews*** are carried out in the form of semi-structured interviews, and cover specific issues on the course content. The data gathered from expert opinions mainly provide answers for research question 1.
- ***Learner reflections*** are obtained by semi-structured interviews with students who enrolled in the course. The data collected through the learner reflections mainly provide answers for research questions 1-b, 2 and 3.
- ***Field notes*** are taken by the researcher during the whole research period, including the course sessions to keep the record of the activities, events and other characteristics of an observation. The data gathered by field notes mainly provide answers for research questions 1, 2, 3.

Table 3.4. *Method Matrix of the Research Questions and Methods*

Research Question	Data Sources	Trustworthiness
R.Q. 1. What are the key factors during the design and development of a course in an attempt to raise the pre-service teachers' information security awareness and cyberethics sensitivity?		
a. What are the content related issues?	Expert interviews and Review of Survey Studies Field notes Designer Reflections Learner Reflections	Data Triangulation Researcher Triangulation
b. What are the learner related issues?	Field notes, Designer reflections Learner reflections	Data Triangulation Researcher Triangulation
c. What are the instruction related issues?	Learner reflections Field notes, Designer reflection	Data Triangulation Researcher Triangulation
R.Q. 2. What are the possible influencing factors for the design, development, and implementation process of the course?		
a. What are the facilitating factors?	Field Notes, Learner reflections, User Reflection	Data Triangulation Researcher Triangulation
b. What are the challenges and how are they handled?	Field Notes, Learner reflections, User Reflection	Data Triangulation Researcher Triangulation
R.Q. 3. How do pre-service teachers perceive the contribution of the course on their information security awareness and cyberethics sensitivity?	Learner reflections, User reflection	Data Triangulation Researcher Triangulation

- ***Designer reflections*** are collected through weekly logbooks. It includes the critical details that occurred during the preparation process of the course content and web environment of the course. In addition to interviews with experts and students, field notes focusing on critical points and the challenges during the design period are logged by the researcher. These data also guided the study. The data gathered by designer reflections mainly provide answers for research questions 1, 2, and 3.

The method matrix of the research questions and methods are presented in Table 3.4.

3.6.1. Expert interviews

The outline of the course and the content pool was generated with the contribution of expert interviews. Before interviewing the experts, the researcher reviewed the literature for identifying the specific needs for information security awareness and cyberethics sensitivity. The broad content pool is constructed. The overall program contained some of the most frequent security incidents such as phishing, virus, hardware crash device and identity theft, peer to peer sharing, and cyberbullying through e-mail. Plagiarism and digital cheating, copyright infringement, oversharing issues are also included from the related literature.

Then, the draft content sequence is presented to experts to gather their opinions and suggestions. The information security experts, who work in the Information Security Unit, Computer Center, suggested the inclusion of "untrusted network" and "secure connection." A faculty member from the Department of Philosophy contributed to the cyberethics contents and suggested the inclusion of "free speech" and "hate speech." A specific type of oversharing, namely "sharenting" is another added topic after an interview with an expert in an Educational Faculty. She also suggested the issues of social media literacy, such as clickbait and hoax.

Having all these reviews and interviews done, the first draft of the course syllabus is proposed to the Faculty Council. It is presented in Appendix B.

3.6.2. Learner Reflections

The learner reflections gathered from two sources of data. They are interviews and observation. Semi-structured interviews with the students was a part of the learner reflections. At the end of each semester, the researcher conducted interviews with the students who voluntarily accepted to participate. The interview schedule is presented in Appendix C. The questions were about what they have learned from this course, whether they knew any topic before and their perception about the contribution of this course to their teaching profession.

During the implementations, the students shared their opinions about that week's contents, exams, or overall design of the course. Their questions about misunderstood or poorly understood topics also have advisory value for this study. Their questions about the contents and feedback about the course were the unstructured parts of the learner reflections.

3.6.3. Designer Reflection and Field Notes

Designer reflection includes the weekly notes taken by the researcher about each lecture session. The notes about the development of the online environment of the course throughout the semester are also part of designer reflections. The preparation of lecture notes, selection of reading assignments, generating and moderating the discussion forums in the online environment of the course, preparation and evaluation of exams were all the elements of the course design process.

Field notes include the observation of the implementation of each lecture. The participation of the students to the lectures, their comments and questions, any technical incidence, and the discussion details were included in the field notes. Their feedback about the course was also considered as field note.

Although both field notes and designer reflections are taken by the researcher, at this point, it is necessary to highlight differences between field notes and designer reflection. The distinction between them is that the content of designer reflection is developed from the experiences in lecture preparation process whereas the field notes are grown according to the observations about the lecturing process, during the class

hour. The learners' experiences and researcher's interaction with them is also part of the field notes.

3.7. Data Analysis Procedures

The researcher obtained qualitative data from the expert interviews, her designer reflections and field notes, and the interviews. Expert interviews were contributed to the needs analysis phase of the study. Designer reflections were taken in a notebook for each incidence for weekly course design period during the implementation process. The online or printed sources used for the course, the lecture preparation process, decisions made by the researcher were all included in designer reflections. Field notes were all observed data during the lectures, the students' responses and weekly contributions in discussion sessions.

The responses of the interviewees were recorded in the interview process. Later, the recorded data were transcribed word by word. The contents of the expert interviews, the notes, taken as designer reflections and field notes were combined with the transcribed student interviews.

Analysis of the qualitative data consists of three progressive actions, data reduction, data display and conclusion drawing processes (Miles & Huberman, 1994). All qualitative data gathered during the study is coded. The codes were compared with a reviewer in order to provide inter-coder reliability. The mismatched codes were rearranged and finally a consensus obtained in the codes. The themes, sub-themes and the related codes are presented in Appendix D.

In the following step, themes are identified and organized according to the major ideas of questions in order to display data. Since the same interview guide is applied to each participant, their responses were relevant to the subject and easily compared in terms of the emerged themes. The consequences of themes were reviewed concerning the research questions in order to permit conclusion drawing.

3.8. Researcher's Role

The researcher of this study is an experienced employee in the computer center of a state university. As a part of her job description, she observed and experienced

several security incidents and took necessary action in such cases. Password and identity theft, privacy issues, ethical use of public ICT resources, and web contents including copyright violation issues were some of the most frequent incidents. In light of these experiences, she developed several policy statements and procedures to regulate the workflow in her institution.

The researcher observed that information security and cyberethics issues were poorly handled in the curriculum of teacher training institutions. For this reason, a course aiming at raising prospective teachers' information security awareness and cyberethics sensitivity was designed. Throughout the study, in addition to being an experienced person in cybersecurity-related topics, the researcher took several roles including teaching assistant of the course, observer, course designer, and developer. In the following sections, these roles are described in detail.

3.8.1. Designer and Developer of the Course

In the design-based research process, firstly, the needs analysis was carried out for compiling the potential topics of the course. For the pre-implementation phase of the study, the researcher developed and arranged the syllabus and the outline of the course. For the first and the second implementations, necessary rearrangements on the content sequence were done by the researcher.

3.8.2. Observer and the Teaching Assistant of the Course

The researcher prepared the contents and audio-visual learning materials for each lecture. In addition to being a designer and developer of the course, the researcher observed the experiences of the instructor of the first implementation and collected data with observation and reflection notes for the next implementation.

For the two implementations, the researcher prepared four mid-terms and two final examinations. Furthermore, the researcher administered the discussion forums on the online environment of the course and facilitated the face to face discussion sessions each week following the lecture session.

Based on the evaluation gathered in the pre-implementation and the first implementation phases, the researcher reported the findings and conducted the required interventions for the second implementation.

3.9. Trustworthiness

The trustworthiness of research is necessary to ensure the reliability and validity of a qualitative research study. In quantitative research, reliability and validity would be evaluated with measurable metric results. On the other hand, for the qualitative studies, to ensure reliability and validity of the results different measures are necessary. Guba (1981) stated four main aspects of trustworthiness, which are; (i) credibility, (ii) transferability, (iii) dependability, and (iv) confirmability. Shenton (2004) and Guba (1981) suggested the following strategies to ensure the first four criteria.

Credibility refers to internal validity and deals with the accuracy of the findings (Guba, 1981). In qualitative research, the results may be affected by the researcher (Shenton, 2004). For this reason, to deal with biased threats, the researcher used various sources of data and applied expert confirmations throughout the study. The findings from different sources of data were continuously triangulated to ensure credibility.

Transferability refers to external validity/generalizability. In a quantitative study, the concern lies in applying the results to a broader population. However, the nature of qualitative research may lead to binding to the study. The generalization of the results of a qualitative study is an argued part among qualitative researchers (Guba, 1981, Shenton, 2004).

The themes that emerged from the study is limited to a specific context and a small group of participants. As a result, it may not be possible to generalize the results to a wider population, or extended context of the study (Shenton, 2004).

The main objective of the study is to design and develop a course to raise pre-service teachers' information security awareness and cyberethics sensitivity. As a result, the context of the study is limited to a particular topic and a well-defined

population group. The generalization of the study can be offered to different participation groups in a similar context.

Dependability refers to reliability. For quantitative research, reliability ensures the replicability of the study with the consistency of the results (Guba, 1981). In a qualitative study, one of the main dependability measures is to express all the details and limitations of the study clearly. To ensure the reliability of the results, in a qualitative study, the analysis of qualitative data is conducted by another researcher and compared each other (Shenton, 2004). In this research, the analysis of the qualitative data is validated with another colleague. The themes that emerged from the interview data are verified with another researcher.

Confirmability refers to objectivity. It is defined as the degree of neutrality of the findings (Guba, 1981). It ensures that the results are based on participants' responses without any external effects, or potential biases or any other factors.

The critical threat to confirmability in this study was that the role of the researcher was perceived as the instructor of the course by the enrolled students. For this reason, the interviews were applied after the grading announced.

The researcher used different data collection methods and sources. In the analysis phase, the draft content pool was constructed according to the literature, and then rearranged as a course outline with expert interviews.

In the design and development phase, the major data collection instruments were the designer reflection and learner reflections. The different sources of data were utilized during the research. The interviews and reflections provide qualitative data. The researcher triangulated the obtained data with each other and exam results.

3.10. Limitations of the Study

This study has methodological limitations. The researcher both designed, developed and implemented the course. Besides, she collected the observation data as field notes of the study. Nonexistence of an external observer was a limitation. The students, registered to CEIT215, were both the learners and the source of data of the study with their feedback and course-related participation.

Reflections and responses of interviewees depend on the time of the feedback and also the students' mood. This issue might affect students' responses in the interviews. They might have expressed their opinions in a more positive or negative way. In order to control this, the researcher took the following precautions; (i) interviews are done after the submission of grades and (ii) the importance of the interviews for the improvement of the course and the academic study was explained in detail at each meeting. The explanation about the research in the first meetings of each implementation help minimizing this threat.

During the implementation, the lecture contents were selected from various sources. The nature of the research required the development of a course from a wide variety of sources. The selection of these sources for each week was limited by the capacity of the researcher to compile them. In fact, due to time limitations, the lectures except for the cybersecurity-related ones, could not be reviewed by experienced instructors.

The online environment of the course was prepared in an online course management system (CMS), namely Moodle. The efficiency of the use of CMS depends on the researcher's competence in the tool. The researcher uploaded the course materials, lecture notes, recommended links, extended lecture notes, for the second implementation, and managed the forum discussions.

The findings of the study are limited to the context of the study. Therefore the researcher should be conscious about interpreting the results of this research (Berg, 2009).

3.11. Ethical Considerations

The researcher applied for approval from the Human Subject Ethics Committees (HSEC) in Applied Ethics and Research Center (AERC) at the beginning of the study. After receiving approval, she conducted several semi-structured interviews with enrolled students, colleagues, and subject matter experts. All interviewees participated in these stages of the research were informed about the nature and the purpose of the study. The ethical approval of HSEC is presented in Appendix E.

The students' contributed to this study in two ways. All the enrolled students were the natural participants of the design-based study since they attended lectures, participated in class or online activities, exams, and other course-related actions. As a part of the field notes, the researcher observed their questions, additional opinions during the lecturing period, and their feedback about that week's contents and collected data for field note. Their contribution to the study was limited to being a CEIT 215 student. The students enrolled in the courses in 2017-2018 Fall and 2017-2018 Spring semester are informed about the course is a part of a research study.

Another contribution of the students was being the interviewee. At the beginning of each interview, the researcher informed about the ethical procedures. She briefed the purpose of the interview, underlined the confidentiality of their responses, preservation of the anonymity of the participant, and informed that the participant was free to leave the meeting any time during the interview. The conversations were recorded with the voice recorder with the permission of the interviewee. Each participant had a name code which referred to the implementation and order of the interview. For example, M206 refers to the sixth interviewee from the second implementation. The names of the participants kept confidential.

CHAPTER 4.

FINDINGS

Throughout the chapter, firstly, the design of the research environment, including the analysis, development and iterative implementation phases, is presented. Later, the themes that emerged from the qualitative analysis are interpreted. The purpose of the study was to explore:

(i) The key factors during the design and development of a course in an attempt to raise the pre-service teachers' information security awareness and cyberethics sensitivity,

(ii) The facilitating and challenging factors that influenced the implementation process, and

(iii) The perceived contributions of the course on the pre-service students' information security awareness and cyberethics sensitivity.

The sources of data were the expert interviews, designer reflections, field notes, and the interviews with the students of both implementations. Design-based research methods were employed in the scope of these purposes. All qualitative data are analyzed and interpreted. The themes that emerged in data analysis are presented in Table 4.1.

Table 4.1. *Themes and Sub-Themes Obtained from the Research Study*

Themes	Sub-Themes	RQ
Design issues	In relation with • Content • Learners • Instruction	RQ1
Challenges and facilitators	In terms of • Instructor • Learners	RQ2
Potential Contributions of the course	• Newly learned topics • Corrected misconception • Raised awareness on C3 • Perceived contribution to the teaching profession • Direct effect on the daily lives of the students	RQ3
Suggestions	• Content suggestions • Instructional Design Suggestions	RQ1

The findings emerged under the themes *Design Issues*, *Challenges and Facilitators* and *Potential Contributions of the course* are explained in Sections 4.2, 4.3, and 4.3.4 respectively. The findings of the *Suggestions* theme, which includes the suggestions from the interviewees and the experiences the researcher had during the research process, were grouped under the content, learner, and instruction related suggestions presented in the corresponding sub-section.

4.1. Design of the Research Environment

Education faculties are teacher training institutions. It is essential that pre-service teachers are educated as well-trained digital citizens with a high level of information security awareness and cyberethics sensitivity. The information security training strategies are either at cybersecurity level, which is the concern of information technology employees rather than the end users or limited to few threats instead of giving an overall information security awareness. For this reason, the topics related to cyberethics and information security were covered in the course. Besides; raising awareness on cyberethics and cybersafety issues are directly related to information security issues.

In the analysis phase of the study, the reports about information security incidents of the computer center of a state university were reviewed. The content selection process and emerged topics are explained in detail in Section 2.2. Besides, in addition to the security incident reports, the recent studies investigating the users' information security awareness and cyberethics sensitivity were reviewed. These studies were selected according to the research focus. In particular, the studies which focus on end users' information security and cyberethics issues were compiled. In this phase, the ICT related needs of the pre-service teachers were tried to be identified. The topics were listed. According to the result of this article survey, the major issues in information security and cyberethics have emerged. According to the evaluation of the articles and reports, the content pool was prepared. The most frequent information security and cyberethics incidents were also included in the content pool, and a draft of the course outline was developed.

4.1.1. Needs Analysis: Generation of the Content Pool

At the beginning of the study, the researcher investigated existing literature in terms of information security and cyberethics incidences in an educational context. She also conducted semi-structured interviews with computer coordinators in the university and faculty of education. The main objective of this preliminary study was to decide the broad list of potential topics of the course. The items were listed in a content pool.

The faculty members of Computer Education and Instructional Technology, Information Security Experts in Computer Center, and a faculty member having expertise on ethics from the Department of Philosophy were asked for their opinion about the content pool. According to their feedback, the outline was finalized as pilot implementation, proposed to the faculty of education and presented in Appendix B.

The content pool was designed by using the following types of sources;

1. Security reports on critical incidents of information organization,
2. Findings of the survey studies related to security awareness and cyberethics and

3. The training programs regarding information security and cyberethics in other countries.

They are explained in detail in the following sections.

4.1.1.1. Security Reports on Critical Incidents of Computer Center

In the Computer Center of the public university where this study is carried out, there is a computer help desk providing support for the computing problems that end users encounter in their daily work. The administrative and academic personnel, the students and the visitors are regarded as end users. Besides, there are department computer coordinators who also give support at local for informatics issues in the departments. The IS personnel who works in the Computer Center can observe security incidences either through access logs or help desk e-mails. The researcher observed several security incidents throughout her experiences. Informal interviews with colleagues provided rich data for her. Because of the privacy and security concerns, the logs would not be presented explicitly. Instead, the researcher took the most frequent incidents into consideration.

As a result of the researcher's analysis of all these experiences and interviews, the researcher found out that the most common information security incidents were *malicious sites* and *phishing e-mails*. These threats are caused by external sources. The threats of malicious insiders were also taken into consideration. *Illegal file sharing via peer to peer* (P2P) networking is one of the most common information security violations caused by the insiders. It results in not only copyright violation but also causes the network access to slow down.

Another source of information was the security bulletins where the weekly summaries of new vulnerabilities are published. Some of these announcements may include but not limited to a software vulnerability of an online service. Computer Emergency Response Team (CERT) publishes these security announcements. The countrywide source of information is the National Computer Emergency Response Center (USOM). They collect and publish cybersecurity information from worldwide sources. IT professionals, generally, follow these security bulletins. USOM provides guidelines for IT professionals so that they could make the necessary arrangements in

their systems. The benefit of these bulletins is not limited to IT professionals. The end users can also take advantage of the information given in these bulletins. For example, they can find information about the vulnerabilities of a specific software they are using, and they can take the corrective actions described. The observed occurrences, effects, and corresponding course topics were presented in Table 4.2.

Table 4.2. *Security incidents observed in Computer Center*

Incident	Effect	Topic
Identity theft	Disclosure of information Loss of data Loss of credit	Phishing, Password Security
Virus infection	Loss of data Hardware effect	Hardware Security, Malware
Software and OS Update	Virus Attack	Software Security
Illegal use of Peer to Peer (P2P) Network	Virus attack Network interruption	Firewall Ethics, Copyright,
Malicious Web Site	Disclosure of information Virus attack	Phishing, Hardware Security
Secure Web Site	Disclosure of information	Privacy
Bluejacking	Disclosure of information	Mobile Security
Malicious Applications	Loss of data Disclosure of information	Mobile Security
Abusive posts	The decrease in the perception of self-confidence	Cyberbullying

4.1.1.2. Findings of Survey Studies and Reports

The researcher reviewed several survey studies focused on end users' information security and cyberethics issues. The selection of the studies was depended on the following criteria; (i) focus of concern would be the information security or cyberethics issues in the use of ICT and (ii) the participants of the study were the end users. In particular, students either in a K12 school setting or at the university level

were more preferred. In some cases, the studies carried on with end users who were not members of an educational domain but not at IS professional level were also considered. The detailed information about these studies is presented in Section 2.2.1.

4.1.1.3. Training programs on Information Security and Cyberethics

There are several information security training programs most of which are prepared at a level appropriate for IT professionals. In the scope of ISO 27000, there is a specific information security training program for end users as well. This program focuses on a basic level of information security, backup, phishing, and virus threats. Duration of the standard training is 3 hours. The safety issues, cyberbullying, addiction, copyright, and other ethical issues are not included in the program.

Cybersecurity is a popular topic, and it has become a part of graduate degree programs in various universities. However, the focus of the programs is to train students at the expert level IT professional. In other words, these graduate programs are not for plain end users.

To summarize, the content pool of the course was developed according to field notes related to information security tutorials, survey studies on cyberethics and cybersafety and semi-structured interviews with field experts. It is represented in Figure 4.1.

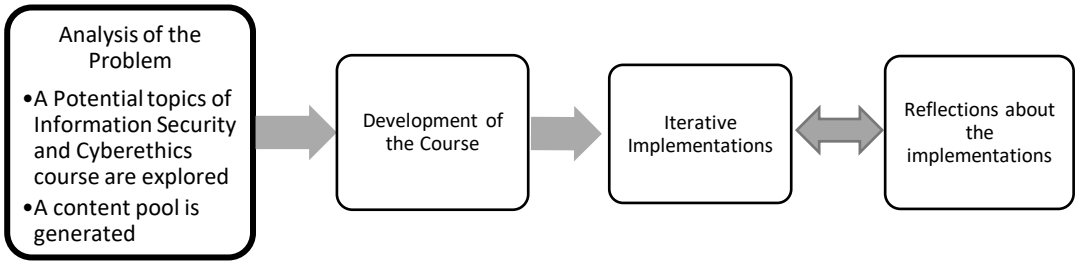


Figure 4.1. Design-Based Representation of the Study – Analysis Phase

Later, as the development phase of the study, the draft outline (Appendix B) was proposed to department instructors, information security experts, and cyberethics specialists. Revising according to their feedback, the outline for the first implementation was finalized. It is presented in Appendix F.

4.1.2. Development of the Course

The course has been developed through three phases; pre-implementation, the first implementation in the Fall Semester, and the second implementation in the Spring Semester.

There was no such course before. For this reason, in the pre-implementation phase, this course was proposed to the Council of Faculty of Education. For this purpose, the selected topics in the analysis part were arranged as a 14-week course syllabus. The course objectives were also included in the course proposal. The course proposal is given in Appendix B. Approval of the Faculty for the course has been obtained.

For the two successive implementations, at the beginning of the semester, the course has been announced to the students. The following means have been utilized for announcements:

- Physical announcements have been posted to the bulletin boards in the Faculty buildings.
- An e-mail has been sent to the student e-mail group of the Faculty of Education.
- Student academic advisors were informed about this course by face-to-face meetings, and they were kindly asked to recommend this course to their students.

4.1.2.1. Development of the Online Environment of the Course

Information security training programs are generally designed for business or information system employees. The cyberethics courses, on the other hand, usually follow *teaching by example* method. In the online environment of the course, several examples about cyberethics, cybersafety and cybersecurity issues were provided to the students. The course content management tool enables the instructors to develop different interaction tools and makes it possible for the students to communicate with each other, with the teacher, with various tools, at different levels.

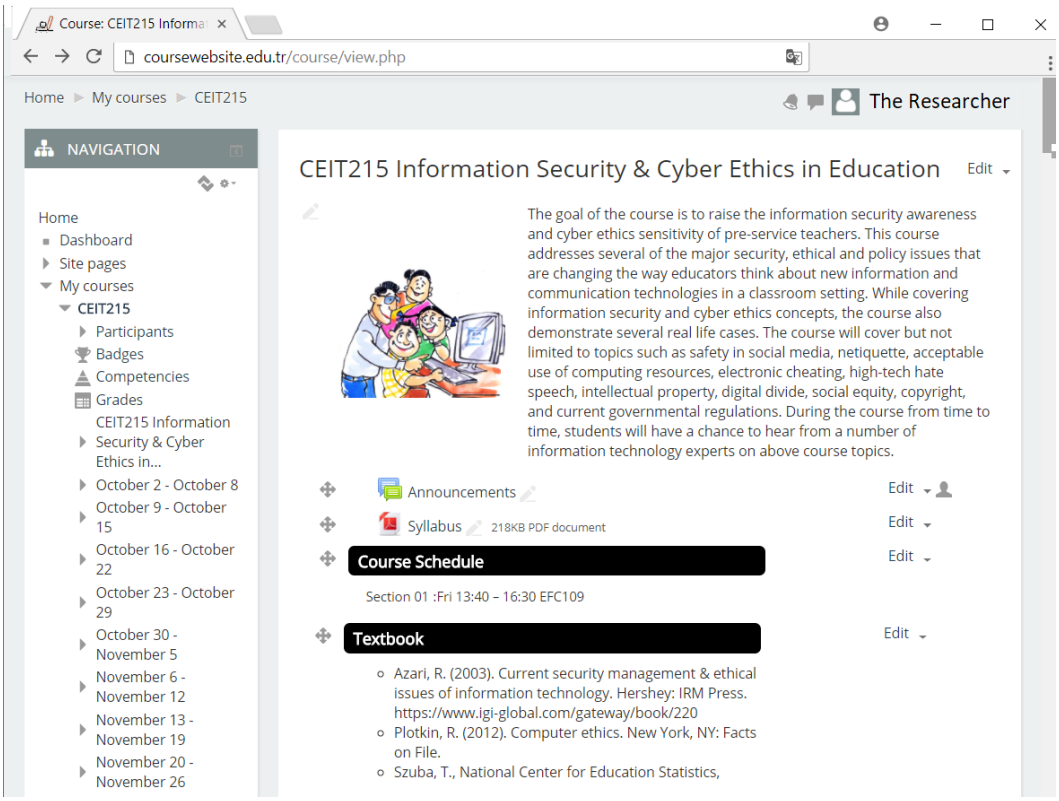


Figure 4.2. A sample screenshot of the course web site

This course is designed to be a blended course with both the support of the online environment and traditional face-to-face sessions. The online environment of the course was developed in Moodle, an open source course, content management system. A sample web site screen is presented in Figure 4.2.

For each week, audio/video materials related to the topic of the week was presented to increase students' attention. The materials include related cases, anecdotal stories, or tutorials. A part of the course web site for some particular weeks, including weekly outline is presented in Figure 4.3.

To summarize; the draft version of the content sequence was created and reviewed by the faculty members, information security experts and computer coordinators of faculty of education. The online environment of the course is developed, and finally, the new course has been announced to the students of the faculty of education. It is represented in Figure 4.4.

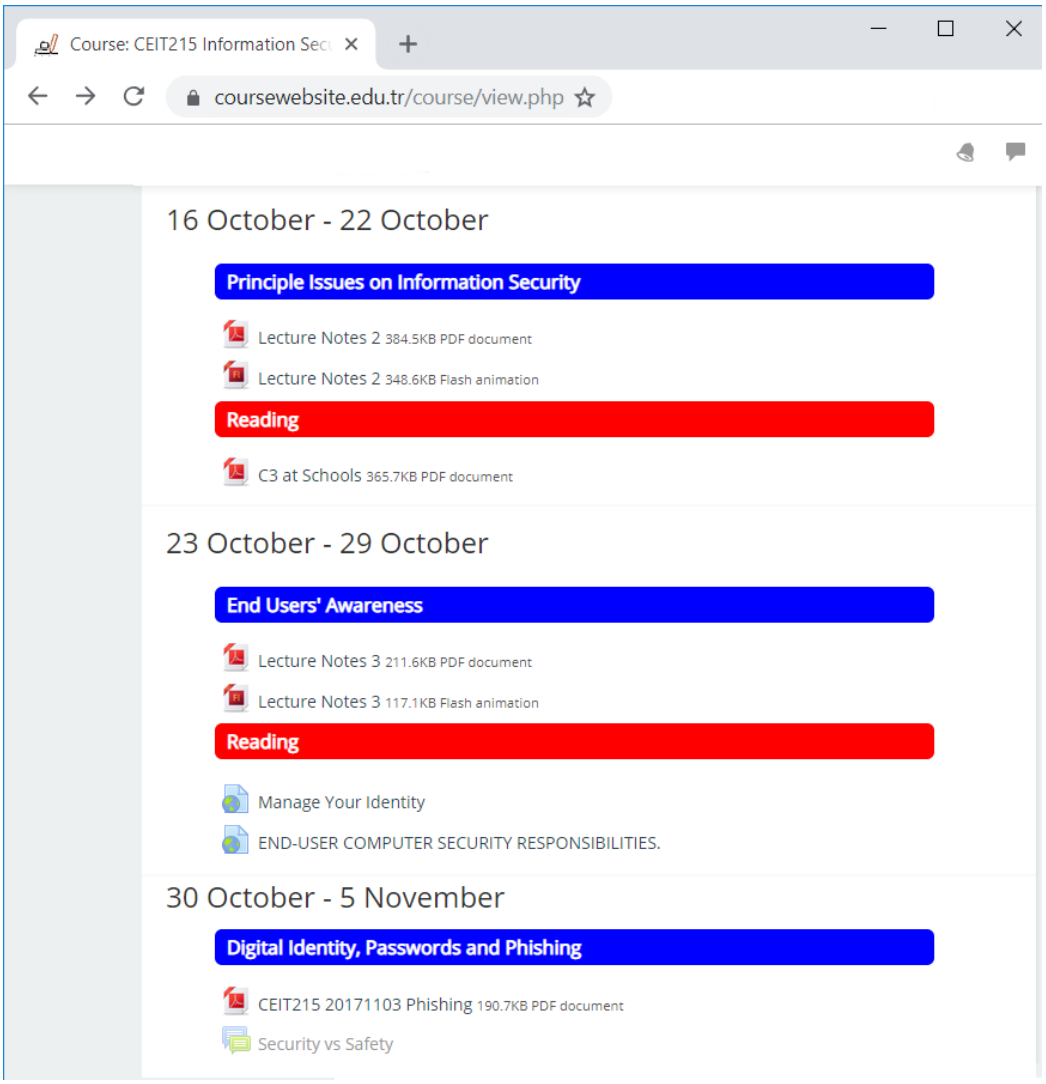


Figure 4.3. A part of the course wall

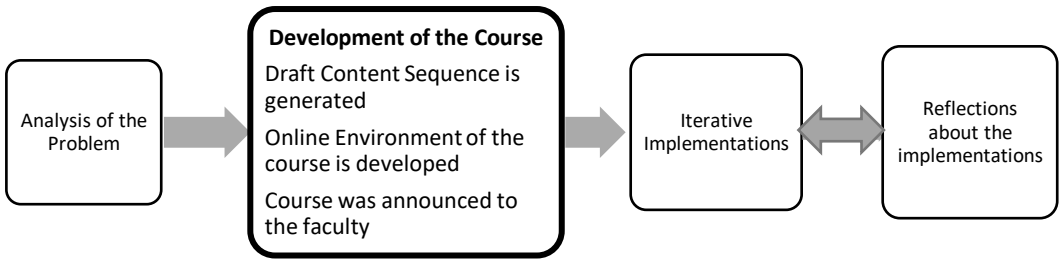


Figure 4.4. Design-Based Representation of the Study – Development Phase

4.1.2.2. The Forum Discussions in the Online Environment of the Course

Another way to encourage the students to think about the topics was to launch forum discussions. The researcher created a forum topic in certain weeks, related to that weeks' course session. A sample of one of the forum pages is presented in Figure 4.5.

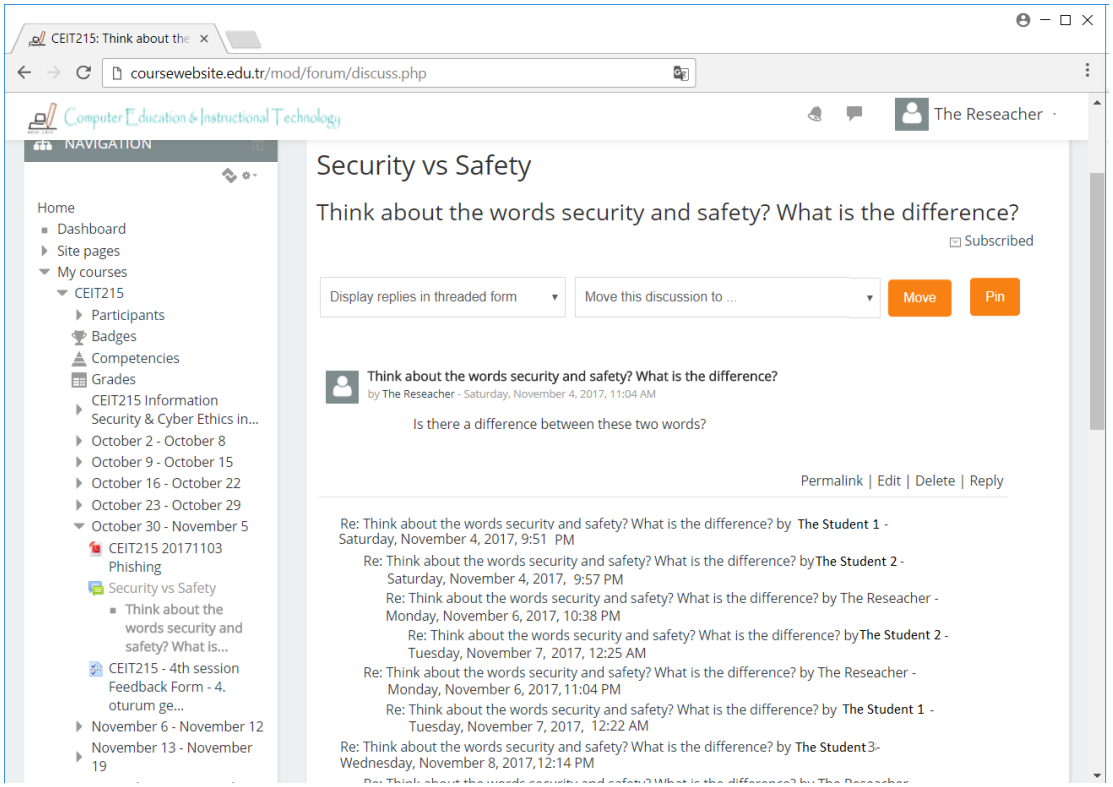


Figure 4.5. A Sample Forum Discussion

4.1.3. Iterative Implementations of the Course

The development process of the course consists of two iterative implementation phases. The course designed by rapid prototyping method for two implementations. The researcher and the instructor redesigned the syllabus, the online environment of the course, and several course materials after each lecture session. The course has 14 weeks in the semester. Two weeks' sessions were the exam sessions. In addition to the 14-week course period, at the end of each semester, a final exam was made.

4.1.3.1. The Registration Period

In the university where this course is given, the students can enroll in the courses through an online registration system. The registration period consists of two stages. The first stage is the registration system, which all students are mandated to enroll at least one course. The second stage is the add-drop period. It is in the second week of the semester. If there is a correction about the enrolled courses, the add-drop activities are performed at this stage, and the registration process is finalized.

The courses, opened in that semester, are defined into the registration system. A course is defined with additional parameters such as course capacity, prerequisite conditions, and the departments to which the courses are open. In some cases, the instructors set the course capacity to zero and carry on course enrollment process through e-mail or face-to-face communication. In that case, the students can finalize registration during the add-drop period in the second week of the semester.

Registration procedures of the course were carried out by the instructor. In the registration period, the course capacity was set to zero, and prospective students of the course were applying by an e-mail including information about their department and their cumulative grade point average (CGPA) information.

The instructor of the course evaluated the e-mail application of the course. One of the primary reasons for this evaluation process was to prevent the unbalanced distribution of the students in favor of Computer Education and Instructional Technology (CEIT) and to ensure the registration of students from different departments of the Faculty of Education. After the approval of the course instructor, the accepted students finalized their registration through the registration system of the university.

At the end of the add-drop registration period, the number of registered students for the first implementation was 40. The distribution of students according to their departments, gender, and year are given in Table 4.3. According to the table; the two major groups were Computer Education and Instructional Technology (CEIT) and Elementary Mathematics Education (EME) students. Four students from Foreign Language Education (FLE) and one student from each one of Chemistry Education

(CHED) and Mathematics Education (MHED) were the other students who registered in the first implementation.

Table 4.3. *Department, Gender and Year Distribution of the Students in the First Implementation*

Department	N
CEIT	22
EME	12
FLE	4
CHED	1
MHED	1
Gender	**N**
M	15
F	25
Year	**N**
2	5
3	20
4	15

The participant selection procedures in the second phase were the same as that of the first phase. At the end of the add-drop registration period, the number of registered students was 21. The decrease in the number of registered students arose from the overlaps in the course schedule. The distribution of students according to their departments, gender and year are given in Table 4.4. According to the table; the participants were almost evenly distributed in CEIT and FLE Departments.

During the registration period, some of the non-CEIT students were concerned about the computer-related difficulty of the course. The researcher arranged the course so that the non-CEIT students could understand. In particular, the cybersecurity-related contents were explained with corresponding non-computer examples as long as it was possible. The specific examples were presented in weekly summaries below.

Table 4.4. *Department, Gender and Year Distribution of the Students in the Second Implementation*

Department	N
CEIT	12
FLE	9
Gender	**N**
M	13
F	8
Year	**N**
2	9
3	8
4	4

4.1.3.2. The First Implementation – Weekly Brief Summary

The course was 3 hours a week, and the schedule was on Fridays at 13:40 – 16:30. Being the last day of the week, the researcher is concerned about the attendance of the students. However, at the end of the semester, it was found that the attendance was higher than the researcher's prediction.

Each week, the contents of the corresponding week were presented to students. The duration of the course presentation was generally less than an hour. The students were able to ask immediate questions. In some cases, the students were asked to provide examples regarding the current topic. Especially, in the cyberethics related sessions, classroom participation increased.

After the first lecture session, the online environment of the course was prepared and launched. In the subsequent weeks, the researcher explained the contents in the first one-hour period of the session. In the second hour, in-class discussions were held. In these discussions, anecdotal details or examples about the topics were explained. The students contributed to their own experiences. They were asked if there were any topics they wanted to be clarified. Two midterm exams and a final examination were administered.

Throughout the semester, the feedback from students was continuously solicited while researcher reflections were jotted down. Based on these feedback and reflection, the researcher modified the order of the contents.

4.1.3.2.1. The First Session

In the first meeting, in order to attract the attention of the students, a puzzle covering the major information security and cyberethics topics were prepared and handed into the students in the first session. The puzzle is prepared from an online educational resource center (PuzzleMaker, 2017). The puzzle and the hidden words are presented in Figure 4.6.

Figure 4.6. A Word Puzzle about Information Security and Cyberethics

The students were informed about the design-based nature of the study. Later, the course topics were explained briefly. The description of the course including the web site, logging procedures, grading policy, and registration procedures were also explained. The students generally asked about the details on the course regulations such as attendance, grading and homework policy. They were informed that this course was the first implementation of the course and the observed findings would be used in

further implementations. The students who registered to the course would be participants of the study. They were also informed about this detail.

As the first discussion session of the semester, the major and the most popular information security and cyberethics issues were discussed. The realized program of the first meeting was consistent with the syllabus of the course.

4.1.3.2.2. The Second Session – General Information

In the second session of the course, general information about cyberethics and cybersecurity were introduced to the students. In addition to the contents written in the syllabus, namely *Security policy and ethics regulations*, the contents covered in this session included an initial brief about information security and cyberethics.

The terms *information*, *information security*, *information asset*, and *CIA Triad* were introduced to the students and the beginning of the lecture. The conceptual definitions were provided from (ENISA, 2010; ISO, 2009, 2017; Pipkin, 2000). Then, the term cyberethics was introduced with Barquin's "*Ten commandments of cyberethics*. (1992)"

Table 4.5. *Change in the Course Curriculum, the Second Week of the First Implementation*

	Syllabus	**Realized Program**
Week 2 October 13	Security policy and ethics regulations • Case of Middle East Technical University • Case of Ministry of National Education	An introductory brief about information security • Definitions and CIA Triad Ten Commandments of Cyberethics Security policy and ethics regulations • 5651 Internet Law, Article 4 • METU Information Technology Resources Use Policy and • MoNE Information Security Directive
	Description	**Rationale**
	• All C3 terms were introduced to the students.	• The main objective of this session was to give a general idea of cybersecurity and cyberethics.

The lecture session continued with legislative regulations; *5651 Internet Law* (Resmi Gazete, 2007), regulations and directives such as "*METU Information*

Technology Resources Use Policy (METU, 2008)," and "*MoNE Information Security Directive* (MoNE, 2012, 2016)." A summary of the realized program for this session and the difference between the syllabus and the program is demonstrated in Table 4.5.

4.1.3.2.3. The Third Session – Introduction to Information Security

In the third session of the course, the researcher decided to change the syllabus. According to the syllabus, under the main topic "Principle issues on information security for educators," "Use of licensed software," "Security management of information assets," and "Maintenance of software and operating system" were supposed to be explained. Explaining security management concepts requires prior knowledge of information security and risk assessment.

However, the two discussion sessions in the first two weeks indicated that the students had no idea about basic topics of information security such as information asset or security threats. The researcher decided that, before explaining the basis of information security, it would not be possible to explain security management clearly. As a result, the third lecture session included the following subtopics; (i) Information security and major terms, CIA triad, (ii) Security facts, (iii) Risks and attack types, (iv) Hacker types and ethical hackers, (v) Threats, and (vi) Hardware security tips.

Security management of information assets is planned to be explained in further weeks. A summary of the realized program for this session and the difference between the syllabus and the program is demonstrated in Table 4.6.

Table 4.6. *Change in the Course Curriculum, the Third Week of the First Implementation*

	Syllabus	Realized Program
Week 3 October 20	Principle issues on information security for educators • Use of Licensed SW • Security management of information assets • Maintenance of SW and OS	Principle issues on information security • Major terms CIA Triad • Security truisms • Risks and attack types • Hacker Types • Hardware Security tips in education
	Description	**Rationale**
	• SW and HW protection are not explained but planned to be explained in the next sessions	• A detailed explanation of information security is required.
	• Licensed SW was not explained either	• Licensed SW is a copyright issue rather than information security
	• Security management is briefly explained with risk and impact terms.	• Security management requires prior knowledge of information security and risk assessment.
	• "Hardware tips" topic is included.	• To balance the load of the next week, hardware security is included.

Several sources were used for this session. The contents of this lecture are based on the contents of the first chapters of the books "*Computer Security Literacy* (Jacobson & Idziorek, 2016)", and "*The Basics of Information Security* (Andress, 2014)." The terms '*confidentiality, integrity, and accessibility (CIA Triad),'* and '*security truisms'* were explained with different examples. The four main truisms of information security are presented below.

i. Security is a matter of economics
ii. Absolute security does not exist
iii. Security is at odds with convenience
iv. Security should be composed of layers of defenses

They are explained with non-computer examples. Throughout the semester, the researcher reminded these terms in related topics.

In addition to these sources, the examples and detailed explanations of the terms were obtained from the following sources (Greene, 2004; Whitman & Mattord,

2012). The lecture included "*Threat types of information security* (Easttom, 2016; Smith, 2016)" and "H*ardware security and safety in schools"* from the online books (Wikibooks, 2016) and (Szuba, 1998).

4.1.3.2.4. The Fourth Session – End User Awareness

Critical student feedback was obtained from non-CEIT students immediately after the third session. They complained about the technical level of the course was rather high to comprehend. They also claimed that the topics covered in that session were perceived to be very difficult to understand.

Based on this feedback, in the fourth session of the course, end user related security issues were introduced to the students in more detail. The following sources contributed to the contents of the lecture. Definitions of the term *end user* are obtained from (Karlsson & Hedström, 2014; NIST, 2013). *Information, information asset,* and *types of information asset* were defined from the official definitions of (ENISA, 2010; ISO, 2017). The information regarding the *protection of information assets* was obtained from the books "*The Basics of Digital Privacy*" and "*Information security management* (Cherry, 2014; Kritzinger & von Solms, 2010)." The examples and guidelines about "*password protection"* and "*hardware security"* were presented from an online source (ITS, 2017). Non-computer information security has also an important value to prospective teachers since the information they should protect is not limited to a digital source. "*Digital identity"* as an intangible asset is another critical concept for pre-service teachers. Web reference prepared by a university provided a good guideline about the protection of digital identity and data backup.

In the online environment of the course, a guideline (Elekwachi, 2002) for end users is provided to the students. The change in the syllabus for the previous week affected this week's program. On this week the information security concepts were explained from end users' perspective. The information asset types and related protection measures were discussed during the lecture. The change in the syllabus is demonstrated in Table 4.7.

Table 4.7. *Change in the Course Curriculum, the Fourth Week of the First Implementation*

	Syllabus	Realized Program
Week 4 October 27	Hardware security • Physical Security • Virus protection, • Backing up and restoring	End User Awareness • Information asset types • Digital assets • Print-based information assets • Hardware assets • Soft assets
	Description	**Rationale**
	• The security concepts were introduced from end users' perspective.	• Physical security explained the previous week. • Virus protection and back-up information were explained in the protection of soft assets.
	• Non-computer (print-based) information asset is included in the course.	• Non-computer information has a critical value for prospective teachers.

4.1.3.2.5. The Fifth Session – Identity Security

Security and privacy are two major key terms of digital identity management. At the beginning of the lecture, first, the distinction of security and safety concepts was discussed. Later, the first discussion forum topic "*Security vs. Safety*" in the online environment of the course was introduced to the students.

In the previous week, the protection of digital identities was briefly explained in the scope of protection of information assets. This week, the concept of "digital identity" is described in more detail. The term "*Digital Identity"* is defined from two different sources; (i) a broader definition is obtained from (Spacey, 2017), and (ii) then a technical definition is presented from (TechTarget, 2018).

Types of Digital Identity are classified as unique and anonymous identities (Plotkin, 2012). First, unique identities such as governmental or organizational identities are presented and then anonymous, in other words, user-created identities, such as SNS accounts are introduced to the students. At this point, end user threats are recalled, and as digital identity holder, their responsibilities are explained. The protection of digital identities is not only an information security issue but also an ethical responsibility in the scope of digital citizenship.

Password security and *strategies of securing password* are explained. Risks of setting complicated password are explained by *Password Paradox.* In this case, the researcher reminded the security axiom "Security is at odds with convenience."

An example of creating a complex but memorable password is demonstrated to the students (ConnectSafely.org, 2016). Then, the result of writing passwords on a paper is explained with a scene from the movie Harry Potter: Goblet of Fire.

Multi-level authentication is a critical strategy for the protection of the accounts on the Internet. The method of securing authentication is explained from the web interface of some of the SNSs. Among the students, two of the most frequent used SNSs were selected as examples (Facebook, 2018b; Pinterest, 2018).

Spear Phishing is the most frequent end user failure (APWG, 2006; Hanus, 2014; METU-CC, 2014). The examples of fake e-mail or web page aiming at phishing are collected from various sites (Phishing.org, 2018) and (OpenDNS, 2017). SNSs have warning strategies customized according to their interfaces. One of them is introduced to the students (Facebook, 2018a). The general guidelines were presented to the students.

The password topic was the repetition of the previous week with the inclusion of identity types and different authentication information. In the second hour of the session, firstly, students' password management strategies were discussed. Then general ethical concerns of the students were shared and discussed. As an auto critic, protection of digital identities, in particular, password strategies were also explained briefly in the previous week. This week password topic took more place and was explained in detail. For this reason, this topic will be reorganized in the second phase of the course. A summary of the week is presented in Table 4.8.

Table 4.8. *Change in the Course Curriculum, the Fifth Week of the First Implementation*

	Syllabus	Realized Program
Week 5 November 3	Identity theft • Phishing • Passwords protecting	Digital Identity Security • Identity types • Password protecting • Phishing • Multi-level Authentication
	Description	**Rationale**
	• Identity Types and different authentication strategies are included in the course • Password protection is an extended repetition of the previous week.	• A secure password is an essential but insufficient measure for the protection of digital identity • Phishing awareness and increasing privacy settings in digital accounts are also necessary.

4.1.3.2.6. The Sixth session – Mobile Security

Mobile security is defined by (TechTarget, 2017). The most common security problems (Cooney, 2012) were summarized. *Mobile-specific threats* and *the protection measures* were introduced from the book "*Mobile Security and Privacy* (Au & Choo, 2017)." The threats to mobile security, and end users' being more vulnerable to these threats were described. End users' responsibilities and security strategies were adopted from the second chapter of the book (Tully & Mohanraj, 2017).

The strategies of selecting trusted application as well as information about malware applications are explained. *Fake notifications*, *malicious images*, and *physical threats* to mobile devices were also described. The lecture continued with *trusted and untrusted Wi-Fi networks*. *Wi-Fi Sniffing* and *Bluejacking* (Techopedia, 2017) were other mobile threats. The eighth chapter of the book "*Mobile Security and Privacy*" written by Au and Choo (2017) was the primary source of information.

Briefly, mobile security issues, threats, and protection methods are explained in this session. Threats to mobile security, application-level threats and precautions, web-level threats, fake notifications, physical threats and precautions, battery safety tips, untrusted Wi-Fi, and safety and privacy of data were the subtopics of the week.

In the discussion part of the session, privacy issues of the applications were discussed. The researcher asked students the number of applications they installed on their mobile devices. When installing an application, the users were forced to approve access to many permissions most of which are seem to be unnecessary. The researcher also asked if they check the type of permissions do they allow while installing an application. Another privacy concern of mobile applications was the fact that they collect our private information. The risk of a privacy breach and the perceived benefits of those applications were discussed.

This weeks' lecture contents were completely different from the syllabus. The main rationale of the difference was that the contents of this week, *Ethical hacking* was explained in the third session. Social engineering might be a part of either ethical hacking or malicious human threat. Human threats were also described in the third week. The malicious threats, such as phishing e-mail or web sites, malware applications were also demonstrated in the fourth and fifth weeks. The mobile version of these threats was also clarified in the sixth week. A summary of the session, description, and rationale of the change in the syllabus are presented in Table 4.9.

Table 4.9. *Change in the Course Curriculum, the Sixth Week of the First Implementation*

	Syllabus	**Realized Program**
Week 6: November 10	Ethical hacking • White-hat hackers • Social engineering	Mobile Security • Critical issues on the use of Mobile devices • Threats to mobile security • Trusted applications • Permissions of applications • Untrusted networks
	Description	**Rationale**
	• The security concepts continued with mobile devices. • Battery safety tips were also included.	• Ethical hackers were described in the third week. • Social engineering related issues were described in previous weeks.

In the online part of the course, three documents were given as a reading assignment. The first one of them is; "*Guidelines for managing the security of mobile*

devices in the enterprise (Souppaya & Scarfone, 2013)" which is a governmental document in the US, aiming at providing a general guideline for the use of mobile devices. The second reading material was a web reference; "*Top 10 ways to secure your mobile phone* (Zamora, 2016)." It provides a brief reference for the end users. The last one is a newspaper article; "*Finders of lost phones* (Gahran, 2012)." The article summarizes Symantec's report and highlights that nearly 95% of the finder of loft phones try to access sensitive information in the found device.

4.1.3.2.7. The Seventh Session – Overall Summary

A general summary of information security concepts was covered. The lecture session included the following topics as outline: (i) Definitions of information security, (ii) CIA triad, (iii) Information security principles, (iv) Types of information assets, (v) Threat types and impact of threats, (vi) Hacker types, (vii) Hardware, software and digital identity security, (viii) Security issues of non-computer information assets, and (ix) Privacy.

A mid-term exam was scheduled for the further week. For this reason, this session was planned to be a "Question & Answer" session. The students asked their questions. Some of the questions were about the attack and hacker types. In the online environment of the course, the information security scenarios were asked in a discussion forum. In the discussion part, the students shared their different information security incidents.

According to the syllabus, mobile security would be covered this and the next week. The syllabus was arranged so that the mid-term exams would not be scheduled on course time. The mobile security contents were explained in the previous week. A summary of the session, description, and rationale of the change in the syllabus is presented in Table 4.10.

Table 4.10. *Change in the Course Curriculum, the Seventh Week of the First Implementation*

	Syllabus	Realized Program
Week 7: November 17	Mobile Security • Critical issues on the use of Mobile devices • Trusted applications • Permissions of applications	• Overall Summary about Information Security
	Description	**Rationale**
	• The all security concepts covered up to that session were briefly presented.	• The next week the first mid-term exam is scheduled.
	• The students shared their several information security related experiences.	• Mobile security was explained in the previous week.

4.1.3.2.8. The Eighth Session –The First Mid-Term Exam

The exam consisted of 21 multiple choice test questions with one correct and three wrong answer choices. Each question was 5 points. Total points they can get from the exam was 105. The questions were related to general regulations and directives about the use of information systems, ISO-27000 standards, and major information security definitions and principles, human threats, phishing, and mobile security.

4.1.3.2.9. The Ninth Session – Ethical Issues on Teaching Activities

In the ninth week of the semester, cyberethics issues were covered. Firstly, the terms ethics and cyberethics were presented. The term *ethics* is defined by different sources such as Learner's Dictionary, Dictionary.com, and Merriam-Webster. Although all three definitions describe the same concept from a different point of views, what they point out in common that ethics is a study of dealing with what is right and wrong behavior. The decision between right and wrong, however, may not be easy in some cases. In the lecture, the researcher tried to show this challenge with an example: The Train Dilemma (Wikipedia WikipediaContributors, 2017).

The lecture continued with the definition of *Cyberethics* (CIS, 2017). Barquin's (1992) *Ten commandments of cyberethics* and how it was presented was described in detail. "*Digital citizenship* (Heick, 2013)", "*Nine elements of Digital Citizenship* (Ribble, 2009)", and "*Core Rules of Netiquette* (Shea, 2004)" were the other topics of the session.

In the discussion session, the students' experiences in different ethical concerns or decisions were discussed. In particular, the ethical issues in educational settings were exemplified.

There is not much difference between the syllabus and the realized ninth week program. The nuances exist in the subtopics of the content. The critical difference was the inclusion of a detailed explanation of the term ethics. A summary of the session, description, and rationale of the change in the syllabus is presented in Table 4.11.

Table 4.11. *Change in the Course Curriculum, the Ninth Week of the First Implementation*

	Syllabus	**Realized Program**
Week 9: December 1	Cyberethics in education • Netizenship • Responsibilities on students' privacy, • Online interaction issues from an ethical perspective. • Digital divide and digital equity	Cyberethics in education • Ethics and Cyberethics • Ten commandments and controversial issues • Digital Citizenship and Nine elements of digital citizenship • Netiquette; definition and principles • Ethical issues in Education (discussion)
	Description	**Rationale**
	• Detailed definition of ethics, "Controversial issues of Ten Commandments" and "Nine Elements of Digital Citizenship" are included. • Digital divide and equity were explained in the discussion session.	• A detailed explanation of the term "*Ethics*" is required. • Responsibilities on students' privacy" is planned to be explained in the further week. • Online interaction issues are a part of netiquette principles.

In the online environment of the course, several resources were presented to the students. The first one was a handout, namely "*Teaching Students Right from Wrong in the Digital Age* (Johnson, 2007)." The document provides a brief guideline

and several violation examples to demonstrate and clarify ethically wrong behaviors while using technology. The other resource was a guideline and workbook of "*The Code of Professional Responsibility for Educators in public schools in the US* (Pryor, Martinez, & Pugliese, 2012)." "*The controversial issues of Ten commandments* (Fairweather, 2004)" and *"Digital Citizenship* (Ribble, 2009)," and "*C3 in schools* (Chen & Shen, 2016)" were the other resources as reading assignment.

4.1.3.2.10. The Tenth Session – Intellectual Property

In the tenth session of the course, the researcher continued to cyberethics related topics such as *Code of Ethics*, *Acceptable Use Policy* (AUP), legal issues on *intellectual property*, *software licenses*, and privacy issues in daily lives. The differences between the syllabus and the realized tenth-week program were the inclusion of AUP, code of ethics and the privacy issues. The subtopics of the copyright were generally related to the business setting. A summary of the session, description, and rationale of the change in the syllabus are presented in Table 4.12.

Table 4.12. *Change in the Course Curriculum, the Tenth Week of the First Implementation*

	Syllabus	**Realized Program**
Week 10: December 8	Copyright issues • Intellectual property, • Fair use of digital sources • Software Piracy • License Types	Code of Ethics and AUP Intellectual Property, Copyright, Patent, Trademark • History, First Sale Doctrine, Fair Use, DMCA • License Types and Creative Commons • Anti-Copyright Act, Free SW, and Open SW movements Privacy
	Description	**Rationale**
	• Code of Ethics, AUP, Privacy, and Anti-Copyright Act topics are included. The subtopics of copyright were given in detail	• Fair use of digital sources was explained in Fair Use Policy and creative commons subtopics.
	• Software piracy was not included	• Software piracy, with its security risks, was an information security issue and explained in end user awareness topic.

Intellectual property topic included regulations and statutes of copyright, patent, and trademark. The researcher described the "*anti-copyright act*" and "*free and open source software* (FOSS)" movement. The major source of the lecture was the twelfth chapter of the book "*Information Systems for Business and Beyond* (Bourgeois, 2014)." Besides, the books "*Intellectual Property: Legal and Moral Challenges of Online File Sharing* (Spinello, 2008)" and "*Understanding copyright: intellectual property in the digital age* (Klein et al., 2015)" provided guidance in the design of this week's lecture.

The course started with a definition and description of the terms; *Code of Ethics* and *Acceptable Use Policy*. *METU Code of Ethics* (METU, 2017) was presented as an example. The researcher also provided different examples from other educational web sites. Later, intellectual property and copyright topics were presented. The subtopics *history of copyright, the first sale doctrine,* and *fair use* were introduced.

Digital Millennium Copyright Act (DMCA), and the controversial issues of DMCA were also presented. Patent and trademark are other subjects of intellectual property which were covered in the course.

The researcher introduced the movements against copyright, namely the "*anti-copyright act*" or in other words, Copyleft. Kopimism religion, Creative Commons License (CC), and General Public License (GPL) (Rouse, 2013), Free and Open Source Software Foundations (FOSS) were the common examples of the anti-copyright act. The online sources Copyleft.org, TechTarget.com, and Free-Soft.org, were the sources of definitions and descriptions.

The lecture continued with privacy issues, including the definition of *personally identifiable information* (PII) and *non-obvious relationship awareness* (NORA). The US and EU regulations and restrictions of record collecting in a school setting were presented.

In the discussion part of the lecture, Turkey related legal issues were presented. Throughout the session, the students were able to ask questions and contribute to the lecture by giving proper examples if necessary. An important computer scientist, Mustafa Akgül passed away a few days before the lecture. He had a very valuable

contribution in spreading the use of open source software in the universities and governmental institutions. In the discussion part, his efforts were introduced to the students.

In the online environment of the course; the book section, "*The Ethical and Legal Implications of Information Systems,*" used as a reference book for this week, was assigned as reading assignment. Furthermore; "*Law of Intellectual and Artistic Works,*" shortly Law 5846 (Resmi Gazete, 1951) was also assigned as reference material. The date of enactment of the statute seems to be old. However; the web reference of the statute includes amendments about recent changes and the details about the legal issues of computer resources. Particularly, the second part; "*legal rights of intellectual properties*" were recommended to be read.

4.1.3.2.11. The Eleventh Session – Academic Integrity

In the eleventh session of the semester, academic integrity and dishonesty were the main topics. After a brief description of academic dishonesty (ÖİDB, 2011), the consequences of disciplinary regulations of CoHE (CoHE, 2012) regarding academic dishonesty is explained.

Types of academic dishonesty were presented with examples. For example, "*Darsee Case* (L. Roberts, 1983)" and "*Bengü Sezen Case* (Baum, 2011)" were the examples of fabricated data. In some cases, the students also contributed to the course with their observed experiences.

Specific dishonesty types, *cheating*, and *plagiarism* were explained in more detail. Plagiarism, plagiarism types (WTS, 2017), reasons and prevention strategies (Roberts, 2008), detection methods, and brief information about citation and academic writing were introduced to the students. Honor code (ÖİDB, 2011), was the final topic of the lecture.

In the online environment of the course, a forum discussion was started about a plagiarism incidence in a university, where the two MS theses were almost the same. The researcher asked for the students' comments about this situation.

The following book sections were assigned as reading. "*Digital cheating and plagiarism in schools* (Ma, Wan, & Lu, 2008)" introduces the readers with "*The Net*

Generation" and uncovers the digital cheating incidents in schools. "*Cheating in exams with technology* (K. Curran, Middleton, & Doherty, 2011)" provides brief information about students' changing dishonesty behaviors in the Internet era and provides precautions about digital cheating. Finally, "*Student Plagiarism in an Online World: An Introduction* (Roberts, 2008)" presents detailed information about plagiarism and provides a guideline for both students and instructors about prevention strategies.

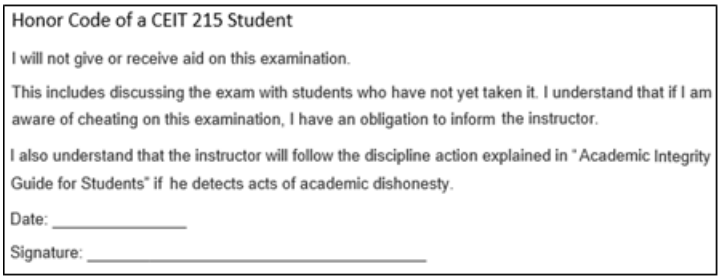
The differences between the syllabus and the realized eleventh-week program were the inclusion of detail information about academic integrity and dishonesty. A summary of the session, description, and rationale of the change in the syllabus are presented in Table 4.13.

Table 4.13. *Change in the Course Curriculum, the Eleventh Week of the First Implementation*

	Syllabus	**Realized Program**
Week 11: December 15	Cheating and Plagiarism • Plagiarism detection software, • Citation issues	• Academic Integrity and Discipline Regulations, • Honor Code, • Cheating, and Plagiarism Types, detection and prevention strategies • Citation issues
	Description	**Rationale**
	• Academic Integrity, CoHe Disciplinary Regulations, Honor Code were included.	• The proposed topics would not be sufficient without providing a proper description of the concept "Academic Integrity."
	• The dominating source of information was the university's academic integrity reference site.	• Reasons for and prevention from plagiarism is a critical issue for the prospective teachers, both for being their students and their future careers.

4.1.3.2.12. The Twelfth Session – The Second Mid-Term Exam

The exam consisted of two parts and one bonus questions. Before the first part, the students were given an honor statement and asked to sign. The honor statement is presented in Figure 4.7.


Honor Code of a CEIT 215 Student

I will not give or receive aid on this examination.

This includes discussing the exam with students who have not yet taken it. I understand that if I am aware of cheating on this examination, I have an obligation to inform the instructor.

I also understand that the instructor will follow the discipline action explained in "Academic Integrity Guide for Students" if he detects acts of academic dishonesty.

Date: _____

Signature: _____

Figure 4.7. Honor Code Statement of the course

The first part of the mid-term exam consisted of 18 multiple choice test questions with one correct and three wrong answer choices. Each question was 5-points. The second part includes seven matching questions. They were 2-points each. The additional bonus was a 6-point question. Total points they can get from the exam was 110. The average grade was 77.45. The highest grade among the students was 100. Only one student got the highest grade.

The test questions were related to cyberethics issues, code of ethics, "Ten Commandments" of cyberethics, copyright issues in the digital world, fair use, patent, privacy issues, plagiarism, academic dishonesty, discipline regulations, and honor code. Digital Netizenship principles were asked with a matching method. As a bonus question, brief information about Mustafa Akgül was given and asked his name to the students.

4.1.3.2.13. The Thirteenth Session – Privacy and Social Network Sites

In the thirteenth session of the semester, some basic cyberethics and cybersafety issues on social media were presented to the students. Mainly, privacy and safety issues of information sharing in social media were explained with the examples of potential harms of oversharing. Sharenting was another major topic of the week. Fraudulent contents in social media were covered with common examples; namely hoax, clickbait, and fake identities. The lecture continued with ethical issues of social media and appropriate and inappropriate usage descriptions.

At the beginning of the lecture, students' social media behaviors were questioned. Then the term *oversharing* is defined from the definition of Dictionary.com. The potential risks of oversharing were presented using audiovisual

sources from YouTube® (Flores, 2014; MSFTOnlineSafety, 2014). These sources provided a visual demonstration about the protection of *digital reputation*, effects of the permanence of *digital footprint* and the critical role of responsible social media behaviors.

Sharenting was another critical cybersafety issue covered in the lecture. It was defined, and the potential risks were clarified (Burridge, 2010). The fraudulent content in social media was described, and *fake profiles, hoax* and, *clickbait* were given as subtopic. How to identify fake profiles was clarified with another audiovisual source (Learn How, 2017). Similarly, clickbait and hoax are the other two most common fraudulent content types. What hoax is and strategies to identify hoax were presented (Christensen, 2017). Clickbait and the major characteristics were explained (Merriam-Webster, 2017) along with some examples.

The lecture continued with *ethical issues of social media use*. Appropriate and inappropriate use of SNS, its effects on digital reputation, and teacher-student interaction issues regarding the use of SNSs were presented. The sources of information were online educational resources from Edutopia (Higgin, 2017), and E-learning Infographics (Teacher Infographics, 2015); and the books "*Lol – omg!: what every student needs to know about online reputation management, digital citizenship, and cyberbullying* (Ivester, 2011)" and the book section "*Information Security and Privacy in Social Media: The Threat Landscape* (Hemamali, 2015)."

The researcher used several resources in this lecture, such as book sections, audiovisual materials, and online resources. The definitions were obtained from dictionary.com and TechTarget.

In the online environment of the course, online resources about sharenting were presented (Steinberg, 2017a, 2017b). An article, summarized several ethical issues on the use of SNS in teaching activities, was another reading assignment of the course (Henderson et al., 2014). A forum discussion is started with the topics *Sharenting and oversharing issues* and *teacher-student interaction in social media.*

There was a radical difference between the syllabus and the realized thirteenth-week program. The change was not limited to the inclusion of the description of

different ethical concepts. Besides, addiction and cyberbullying topics were planned for the following week. A summary of the session, description, and rationale of the change in the syllabus are presented in Table 4.14.

Table 4.14. *Change in the Course Curriculum, the Thirteenth Week of the First Implementation*

	Syllabus	**Realized Program**
Week 13: December 29	Social Media • Malicious profiles, detection, and prevention • Cyberbullying • SNS Addiction	Ethical Issues of SNS • Oversharing and sharenting, • Fake profiles, hoax, and Clickbait • Cyberethics and privacy issues of SNS • Teacher-Student interaction in SNSs.
	Description	**Rationale**
	• Oversharing, sharenting, Hoax, and Clickbait were included. • Student-teacher interaction issues were included.	• Fraudulent content was not limited to malicious profiles Because of the limited duration of lecturing hour, cyberbullying and addiction topics were delayed to the further week.

4.1.3.2.14. The Fourteenth Session – Cyberbullying, Freedom of Speech, and Addiction

In the fourteenth and the last session of the semester, three main topics of cybersafety and cyberethics were covered. *Cyberbullying*, a critical threat, particularly for K12 students, was explained in detail. *Freedom of speech* is a crucial ethical concern especially with the spread of SNSs. Finally, *addiction*, is a safety issue for internet users, particularly for students and children alike. Because of the time limitation, the last two topics were discussed briefly.

First, the term *cyberbullying* is defined (ETCB, 2012; HHS, 2015b; Rouse, 2012). *Types of cyberbullying* were demonstrated (ETCB, 2013). Namely, *harassment, flaming, exclusion, outing,* and *masquerading* were defined. The students contributed to the lesson with their lived or observed experiences. Later, *prevention strategies* (Clifford, 2012; Dikmen, n.d.; HHS, 2015a), *the characteristics of the victims and the*

bullies (Eaton, 2017), and *signs of cyberbullying* (Eaton, 2013; HHS, 2015a) were presented.

The books "*Bullying and cyberbullying: what every educator needs to know* (Englander, 2013)," "*Cyberbullying among children and teens* (Eaton, 2017)" and "*Truths and myths of cyberbullying* (Kowalski, 2010)" were guided this part of the lecture. Besides, the online resources hosted by NGOs were provided brief guidelines.

Freedom of speech is explained with definitions from Merriam Webster and Article 26 in the Turkish Constitution. Then, *hate speech*, a limitation of freedom of speech is described. Addiction-related contents include the definition ("addiction," n.d.) and *types of addiction*. Later, *avoidance strategies* were presented.

According to the syllabus, only the "*Freedom of Speech*" and related subtopics would be explained. However, cyberbullying and addiction were also included. The differences were briefly explained in Table 4.15.

Table 4.15. *Change in the Course Curriculum, the Fourteenth Week of the First Implementation*

	Syllabus	**Realized Program**
Week 14: January 5	Freedom of Speech • Borders and censorship • Auto-censorship • Hate speech, discrimination	Ethical Issues of SNS • Cyberbullying • Addiction • Freedom of Speech
	Description	**Rationale**
	The cyberbullying, addiction, and freedom of speech were briefly presented.	• It was the last session of the semester. However, the topics were worth to be explained at least in a brief way.
	The 1st and the 2nd exams were reviewed in the discussion session.	• Before the final exam; it was a way to cover the poorly understood topics.

4.1.3.2.15. The Final Exam of the First Implementation

The exam consisted of two parts. The first part included 15 multiple choice test questions with one correct and three wrong answer choices. Each question was 5 points. The second part included 15 matching questions. They were 2 points each.

Total points they can get from the exam was 105. The average grade was 86.28. The highest grade among the students was 105. Two students got the highest grade.

In the final exam, all objectives of the course were questioned. The topics of last two weeks, namely ethical issues in social media, sharenting, and addiction, cyberbullying, freedom of speech and addiction with the inclusion of previous topics covered throughout the semester were asked with test questions. The general terms in information security and cyberethics were also asked in another 15 questions matching test.

4.1.3.3. Summary of the First Implementation

Throughout the semester, the researcher utilized several resources, printed or electronic books, journal articles, e-zine and blog sites in order to develop an explicit, detailed course content. To summarize; the course materials such as lecture presentations and reading materials were prepared. The content sequence is redesigned. The online environment of the course was developed. Extended reading materials were prepared for the second semester. There have been differences between the course outline and the realized program. Week based differences and the rationale for these differences are presented in the corresponding subsection. The term based summary of the differences and weekly session summaries are presented in Appendices G and H respectively. The visual demonstration of the study is represented in Figure 4.8.

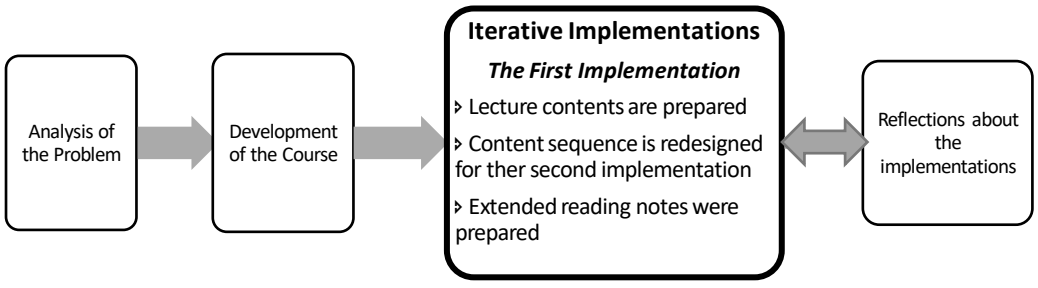


Figure 4.8. Design-Based Representation of the Study – Iterative Implementations: Phase 1

4.1.3.4. The Second Implementation

The schedule of the course was on Tuesday's 12:40 – 15:30. The general characteristics of the course, such as in-class discussions, the language of instruction, and online discussion forums were similar to those of the first implementation. Every week, the contents of the corresponding week were presented to students in a 1-hour lecture session. The students were able to ask any confusing topics or contribute to the lecture by giving related examples.

In the second implementation, two significant changes were made.

a. The content sequence has been changed. The course web site and the course lecture notes were updated accordingly. The differences between the weekly outlines of the first and the second implementations are described in the respective section below.
b. For each session, the content in the lecture presentations was extended, and students were provided with reading notes, and they were required to reading both the lecture presentations and the extended lecture notes.

Significant differences between the two implementations are presented in Table 4.16.

Table 4.16. *Significant differences between the first and the second implementations*

Detail	First Implementation	Second Implementation
Weekly Schedule	Friday 14:00 – 16:00	Tuesday 13:00 – 15:00
Number of students	40	21
Departments	CEIT, EME, FLE	CEIT, FLE
Content Sequence	Appendix F	Appendix I

4.1.3.4.1. The First Session – Introduction

In the first session of the second implementation; initially, general course policy was introduced. The course web site and how to log in to the site were explained in more detail. Later, the first week's topics as in the syllabus were lectured. The major topics of the week were; *Acceptable Use Policy* (AUP) and the *Law 5651*. There were

minor differences between the syllabus and the realized program of the course. A summary of the topics of the week is presented in Table 4.17.

Table 4.17. *Change in the Course Curriculum, the First Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 1: February 13	• Course regulations and General details. • Registration issues.	*General Information about the Course* • Course regulations and • Registration issues. • Description of the course website
	IT Use policy and ethics regulations • AUP and METU IT Resources Use Policy and MoNE directives • 5651 Internet Law, Content Providers	*Acceptable use policy* • METU IT Resources Use Policy • MoNE IT and Security Directives Law5651, Content Providers
	Description	**Rationale**
	Logging issues of the course web site were explained in detail.	The SSL certificate warning of the web site is explained in detail.
	AUP was the main topic of the lecture.	• METU IT use policy and MoNE regulations were presented as examples of AUP. • Besides the ToS of the online resources were given as examples.
	The students' concerns and expectations were questioned.	Their responses gave an idea about the further weeks of the course

Similar to the corresponding week of the first implementation, METU IT Use Policy and MoNE's Security Directives for the teachers were presented as examples of AUP. During the explanation of Law 5651; the term *content provider* and related regulations were explained in more detail. At the discussion session of the first week; students' expectations from and concerns about the course were asked.

In the extended reading notes, the same topics explained in the lecture were presented in more detail. The term AUP was defined by different sources. The MoNE circular on the use of social media was added to the reading notes. The sources used in the reading notes were the books "*Information Systems for Business and Beyond*

(Bourgeois, 2014)" and "*The Internet and the Law: What Educators Need to Know* (Conn, 2002)" and legal statutes and regulations such as Law 5651 (Resmi Gazete, 2007), METU's and MoNE's Policies (METU, 2008; MoNE, 2017a) and MoNE Social Media Circular (MoNE, 2017b).

4.1.3.4.2. The Second Session – Cyberethics and Digital Citizenship

In the second session; the general ethical issues were introduced. Namely, the terms *ethics*, *cyberethics*, and *digital citizenship*, *digital footprint*, as the primary indicator of online reputation, were described. The lecture topics were not different from the syllabus. The minor differences and a summary is presented in Table 4.18.

Table 4.18. *Change in the Course Curriculum, the Second Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 2: February 20	Ethics and cyberethics • Ten commandments and controversial issues Netizenship and netiquette	Ethics and cyberethics • Ten commandments and controversial issues Digital Citizenship and netiquette Digital Footprint
	Description	**Rationale**
	The topic "Digital footprint" is included.	Online reputation is a critical issue for internet users, including pre-service teachers. A digital footprint is an essential indicator of online reputation
	Legal, moral and ethical concepts were discussed.	Being able to identify and discuss ethical and legal issues about online issues is a part of the course objectives.

In contrast to the fact that *cyberethics* was explained in the ninth session of the first implementation, in the current session. Similar to that of the first implementation, the term "ethics" is defined, and the train dilemma was given as an example of ethical conflict. The term cyberethics, and Barquin's (1992) "Ten Commandments of Cyberethics" were presented. Later, the terms "*netiquette* (Shea, 2004)", "*digital citizenship* (Ribble, 2009)", and "*digital footprint* (Kuehn, 2012)" were elucidated. The last topic, digital footprint, was the reading assignment in the first implementation. At the discussion session, legal, ethical and moral concepts were compared. Contradicting or supporting examples were asked.

In the extended lecture notes, in addition to the detailed explanations of topics covered in the lecture, the differences and intersections of the terms; *law, ethics* and *moral* were presented. Fairweather's (2004) argumentation about "*Ten commandments of cyberethics*" was included. It was assigned as reading in the first implementation. Finally, *digital footprint* was explained.

Using different resources, the researcher tried to explain the effects of digital footprints on privacy and reputation of Internet users. Several resources such as dictionaries (Oxford, Merriam Webster, Encyclopedia of Sciences and Religions), audiovisual resources (YouTube), e-zine (Internet Society, Teach&Thought, and Teacher News Magazine), online resources (EdTechPolicy, DigitalCitizenship.net, ethics.org) and e-books were utilized for explaining cyberethics.

In the online environment of the course, the students were asked to describe and compare legal, ethical, and moral concepts. They were also asked to give examples which support or contradict each other. In addition to the extended lecture notes, the following articles were assigned as reading; (i) *Commentary on the "Ten Commandments for Computer Ethics* (Fairweather, 2004)", (ii) "*Manage Your Digital Footprint* (Kuehn, 2012)", (iii) "*To be or not to be: the Importance of Digital Identity in the Networked Society* (Costa & Torras, 2012)" and (iv) "*Netiquette* (Shea, 2004)."

4.1.3.4.3. The Third Session – Code of Ethics and Academic Integrity

In the third session, general concepts about the *code of ethics* and *academic integrity* were delivered. The lecture outline consisted of the following topics: (i) *Code of Ethics*, (ii) *Academic Integrity*, (iii) *Honor Code*, (iv) *Academic Dishonesty*, (v) *Types and Consequences of Academic Dishonesty*, (vi) *Plagiarism*, and (vii) *Digital Cheating*.

Before the syllabus change, the topic "Academic integrity" was lectured in the eleventh session of the first implementation. The code of ethics was explained in the tenth session. There was not any difference between the syllabus and the realized program except for the discussion session of the course. A summary of the course week is presented in Table 4.19.

Table 4.19. *Change in the Course Curriculum, the Third Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 3: February 27	Code of Ethics and Academic Integrity • Honor Code and Discipline Regulations, • Cheating • Plagiarism Types and Citation issues	Same as the syllabus
	Description	**Rationale**
	The dishonesty types were discussed with examples.	The students' observed experiences enriched the course
	The reasons for self-plagiarism were explained in more detail.	It was noticed that the students have a misconception about Self-plagiarism

The course started with the definition of *code of ethics* (Bourgeois, 2014). METU Core Values (METU, 2017) was given as an example. Honor Code (Oxford) was defined. Academic dishonesty, rewards of academic integrity, consequences of academic dishonesty, and disciplinary regulations of CoHE were described. Similar to that of the first implementation, the types of dishonesty were explained by examples and lived experiences. The students' contribution enriched the contents.

In the online environment of the course, two forum discussion topics were launched. In the first topic, the students were asked to write a code of ethics statement by positioning themselves as managers of an educational institution. In the second forum discussion; a plagiarism incidence in a university was demonstrated, and the researcher asked the students' comments about this situation. The latter one was asked in the first implementation also.

In the recommended reading section, not only the reading assignments but also the online references were provided to the students. "*Digital Cheating and Plagiarism in Schools* (Ma et al., 2008)", "*Cheating in Exams with Technology* (K. Curran et al., 2011)", and "*Student Plagiarism in an Online World: An Introduction* (Roberts, 2008)" were the resources given in the first implementation. In the second implementation, the chapter "*Bilingual Plagiarism in the Academic World* (McNaught & Kennedy, 2009)" was included in the recommended readings section. Furthermore, "*The Academic Integrity Guide of METU* (ÖİDB, 2011)" was given as an example.

In the extended lecture notes, the topics covered in the lecture session were elaborated in more detail. The different examples for *honor code*, *types of academic dishonesty* and *types of plagiarism* were presented. In addition to the dictionaries (Oxford, Merriam Webster) and an e-zine document (Asc.org), the sources in the recommended reading section were used as references.

4.1.3.4.4. The Fourth Session – Copyright and Intellectual Property

In the fourth session of the second implementation, *intellectual property* and copyright-related concepts were introduced. The lecture outline consisted of the following topics (i) *intellectual property*, (ii) *definition* and *history of copyright*, (iii) *fair use exception*, (iv) *Digital Millennium Copyright Act (DMCA)* and *Safe Harbor* provision, (v) *license types*; (vi) *Creative Commons*, and (vii) *Copyleft act* were presented.

Before the syllabus change, the topic "*Intellectual property and copyright*" was lectured in the tenth session of the first implementation. In addition to copyright-related topics, Acceptable Use Policy (AUP), code of ethics, and digital privacy were also covered in that course week. In contrast to the first implementation, in the current semester, as a result of the change in the content sequence, AUP and code of ethics were explained in the second and third sessions respectively. Privacy issues were explained in the sixth week in the second semester, and the details about that topic were presented in the further sections.

In this session, the syllabus and the realized program were quite similar. The difference existed in the exclusion of two subtopics, namely *The First Sale Doctrine* and *Digital Rights Management* (DRM). They were concerns of copyright holders rather than end users. There may be an incidence that a student can be a copyright holder, but this course was designed under the assumption that all students were the end users. A summary of the course week is presented in Table 4.20.

Table 4.20. *Change in the Course Curriculum, the Fourth Week of the Second Implementation*

	Syllabus	Realized Program
Week 4 March 6	Copyright and License Issues • Intellectual Property • Copyright, History, First Sale Doctrine, Fair Use, DMCA, and DRM • License Types and Creative Commons • Anti-Copyright Act, Free SW, and Open SW movements	Copyright and License Issues • Intellectual Property • Copyright, History, Fair Use, DMCA • License Types and Creative Commons Anti-Copyright Act, Free SW, and Open SW movements
	Description	**Rationale**
	"First Sale Doctrine" and "Digital Rights Management" is omitted.	They were not related to the pre-service teachers.
	The students' questions about previous topics were discussed.	The first mid-term exam was in the next week.

The lecture started with the definition of *intellectual property* and *copyright*. The same resources utilized in the first implementation were guided the course design of this week. *Fair use exceptions* were explained with examples from education domain. Copyright issues about digital media were explained under *DMCA* topic. In particular, *safe harbor provision* was a case that the students were more familiar with. The *Anti-copyright movement*, namely the *Copyleft Act* and the examples, such as *Creative Commons* and *Free and Open Source Software* (FOSS) Foundations were also explained as it was in the previous version.

In the extended lecture notes, the terms and examples were presented in more detail. The dictionaries (Merriam-Webster, Oxford Dictionary), online resources (copyrighthistory.com, Creative Commons, gnu.org, fsf.org) and the e-book (Bourgeois, 2014) were the resources of the lecture notes.

4.1.3.4.5. The Fifth Session – The First Mid-Term Exam

The exam consisted of two parts. The first part consisted of 20 multiple choice test questions with one correct and three wrong answer choices. Each question was 4-points. The second part included ten matching questions. They were 2-points each. Total points they can get from the exam was 100.

The test questions were related to METU IT Use Policy, MoNE Directives, cyberethics issues, code of ethics, ten commandments of cyberethics, METU Code of Ethics, AUP, copyright duration and copyright issues in digital world, safe harbor provision, fair use, patent, creative commons, plagiarism, academic dishonesty, discipline regulations, honor code, and digital footprint. "*The Principles of Digital Citizenship*" were asked with matching type questions.

4.1.3.4.6. The Sixth Session – Safety Issues of the Social Networking Sites

In the sixth session, cybersafety issues were introduced. Firstly, privacy issues with the following subtopics were explained; *Personally Identifiable Information* (PII), *Non-Obvious Relationship Awareness* (NORA), potential threats and international regulations on PII, and *Do Not Track Statement*. Later, social networking sites (SNS) and behavioral privacy threats, such as *oversharing* and *sharenting* were explained. The common media literacy problems, h*oax* and c*lickbait,* were the other important topics of the session.

Before the syllabus change, digital privacy issues, such as PII and NORA were explained in the tenth session. The behavioral safety issues were covered in the thirteenth session in the previous semester.

Initially, the terms privacy, unique and non-unique identifiers, PII, and NORA were defined. The regulations and restrictions of collection of private record and *Do Not Track* statement were clarified.

Before explaining the privacy issues about SNSs, "*social media*" is defined (TechTarget, 2016). Then, privacy threats were listed. Oversharing, sharenting, and risks of sharenting were the critical issues of SNS privacy which covered in the lecture. The fraudulent contents, such as fake profiles, clickbait, and hoax were lectured in the rest of the session. The strategies to identify fake profiles, and recognize hoax contents were explained in detail.

In the discussion session, the proper and improper social media experiences were discussed. The researcher asked the students whether they have any social media account. The educational affordances and risks of these tools were also discussed in the classroom.

In the online environment of the course, the researcher asked the students their opinions about sharenting and its affordances and risks. In the "recommended links" section, the researcher provided different information sources about oversharing, sharenting, and fake accounts. The resources about oversharing include two blog sites from (Nolan 2018), and (Bilton, 2010) and an online reference from (Internet Safety, 2016). The sharenting resources were audiovisual resources from (Steinberg, 2017a, 2017b). The blog pages (AAP, 2016) and (Miller, 2017) highlight the dangers of sharenting on the children. The audiovisual tools published by (Flores, 2014; MSFTOnlineSafety, 2014) highlight the dangers of oversharing. (Learn How, 2017) explained the methods to identify fake profiles.

In the extended lecture notes, the terms and examples were presented in more detail. The legal issues, such as the acts and statutes of personal data protection of EU; "General Data Protection Regulation (EU, 2016)", and Turkey; "Law on the Protection of Personal Data, Law 6698", were included in the lecture notes. Apart from these, related circulars and regulations issued by MoNE and Ministry of Health (MoH) were also included. They are (i) "Publication of Audiovisual Content (MoNE, 2015)", (ii) Social Media Interaction (MoNE, 2017), (iii) Ethical Regulations of Counseling (MoNE, 2017), and (iv) Regulation on Processing and Privacy of Personal Health Data (MoH, 2016).

The syllabus and the realized program were different in a way that, the privacy and legal issues of the protection of private information were included in the lecture. As a result, the topic "Teacher's SNS Responsibilities" was postponed to the next week. A summary of the course week is presented in Table 4.21.

The dictionaries (Merriam-Webster, Oxford Dictionary, TechTarget, Macmillan Dictionary, Collins), online resources from governmental offices, such as the Department of Protection of Personal Information (kvkk.gov.tr), Computer Security Resource Center (csrc.nist.gov), Internet Safety Resource (StaySmartOnline.gov.au), and NGO sites such as Teyit.org and e-book (Bourgeois, 2014) were the resource of the lecture notes. Besides, the legal statutes, regulations, and circulars (MoNE, 2014; MoNE, 2017; KVKK, 2018) were also benefited in the lecture.

Table 4.21. *Change in the Course Curriculum, the Sixth Week of the Second Implementation*

	Syllabus	Realized Program
Week 6: March 20	Safety Issues of the Internet • Teachers' Responsibilities on students' privacy • Interaction issues on social media • Oversharing and Sharenting	Privacy • PII, NORA Privacy issues of Social Media • Threats to Privacy; Oversharing and Sharenting Fraudulent contents • Fake Profiles, Hoax, and Clickbait
	Description	**Rationale**
	Privacy Issues included.	It was the prerequisite topic of social media privacy
	The content "Teachers SNS Responsibilities" was planned to be explained next week	Because of time limitation; this topic was delayed for the further week.

4.1.3.4.7. The Seventh Session – Privacy issues in Education

In the seventh session of the second implementation, the topic *"Teachers' Ethical Use of Social Media"* was introduced in the lecture. One of the major threats for K12 students in the Internet era was *cyberbullying*. In the second part of the lecture, the reasons for and prevention strategies from cyberbullying were taught in detail. Types of cyberbullying, as well as characteristics of bullies and victims, were explained. In contrast to the current semester, the topics *teachers' responsible SNS use* and "*Cyberbullying*" were covered in the thirteenth the fourteenth weeks respectively.

The syllabus and the realized program were different because of the change that occurred in the previous week. "Teachers' SNS Responsibilities" was included in the lecture. As a result, the topic "Addiction" delayed to the next week. A summary of the course week is presented in Table 4.22.

The lecture started with highlighting the increased use of SNSs. In the first part of the lecture, the effects of misuse of SNSs on digital reputation have been reminded. After demonstrating the risks of teacher-student interactions through SNSs, the lecture continued with appropriate interaction methods. As in the previous semester; the sources of information were online educational resources from Edutopia (Higgin, 2017), and E-learning Infographics (Teacher Infographics, 2015); and the books

"What Every Student Needs to Know About Online Reputation Management, Digital Citizenship, and Cyberbullying (Ivester, 2011)" and "Information Security and Privacy in Social Media (Hemamali, 2015)."

Table 4.22. *Change in the Course Curriculum, the Seventh Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 7: March 27	Safety Issues of the Internet • Cyberbullying and social desirability • Addiction	Ethical issues in Social Media • Teachers' Responsibilities on students' privacy • Interaction Methods in SNS Cyberbullying
	Description	**Rationale**
	"Teachers' SNS Responsibilities" was included.	It is critical information for pre-service teachers.
	The content "Addiction" was planned to be explained next week.	Because of time limitation; this topic was delayed for the next week.

In the second part, cyberbullying related issues were explained. As it was in the previous semester, the term cyberbullying is defined and described. The lecture continued with the types of cyberbullying, characteristics of bullies and victims (Eaton, 2017). The same sources of information used in the previous semester were contributed to the lecture contents of this week.

In the online environment of the course, the researcher asked the students their opinions about teacher-student-parent interaction through SNSs. In the "recommended links" section, the researcher provided several resources, namely; (i) "*Teaching Students Right from Wrong in the Digital Age* (Johnson, 2007)," (ii) "*Workbook of Code of Professional Responsibility for Educators in Public Schools in the US* (Pryor et al., 2012)," (iii) "*Ethics of Teaching with Social Media* (Henderson et al., 2014)," and (iv) "*Cyberbullying Among Children and Teens* (Eaton, 2017)."

In the extended lecture notes, the SNS use among K12 students was summarized in detail (Common Sense, 2015). As in the lecture presentation, the main topics, protection of students' privacy, the risks of teacher-student interaction through SNSs as well as proper and improper use of SNSs were elaborated.

In the second part of the lecture notes, the term bullying, cyberbullying, and the types of cyberbullying, such as harassment, flaming, exclusion, disclosure, and masquerading were described. Prevention strategies and characteristics of cyberbullies and victims were explained in detail. This part of the lecture notes also includes a guideline of what to do in case of a cyberbullying incidence.

The dictionaries (Merriam-Webster, Oxford dictionary, TechTarget, Macmillan Dictionary, Collins), online resources (Common Sense Media, Edutopia, E-Learning Infographics, NoBullyiing.com, EndCyberBullying.org, Learning and Teaching Leadership) were utilized as sources of information.

4.1.3.4.8. The Eighth Session – Freedom of Speech

In the eighth session, the major topic was *freedom of speech*. In the first implementation, it was briefly introduced in the fourteenth week. In the current semester, the researcher elaborated the concept of free speech. The following subtopics were added; (i) *symbolic speech*, (ii) *limitations of free speech*, (iii) *hate speech*, (iv) *censorship*, (v) *online free speech issues* and (vi) *special regulations in an educational setting*. The syllabus and the realized program were quite similar except for the inclusion of the phrase *symbolic speech*. A summary of the course week is presented in Table 4.23.

Table 4.23. *Change in the Course Curriculum, the Eighth Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 8: April 3	Ethical issues on free speech through the use of ICT • Borders and censorship • Auto-censorship • Hate speech, discrimination	Freedom of Speech • Free speech, symbolic speech • Limitations of freedom of speech • Hate Speech • Censorship • Speech issues in the Internet
	Description	**Rationale**
	Symbolic speech is included.	In the Internet era, symbolic speech is a more frequent type of speech.
	Freedom of Speech in education was discussed.	The special points to take care in education was critical.

The lecture started with the definitions of *speech*, *freedom of speech*, and *symbolic speech*. The sources of definitions were Legal Dictionary, Oxford, and Britannica. Later, the historical background of freedom of speech was introduced with *First Amendment of the US Constitution*[e]. Later, *Turkey Constitution (Article 26)*[f] and the *European Union (Article 10)*[g] were presented. The lecture continued with the limitations of freedom of speech[h]. Hate Speech, one of the limitations was explained in more detail (Parekh, 2006). Hate crime hoaxes (College Fix Staff, 2017) and a movement against hate speech were introduced (nohatespeechmovement.org). Later, censorship and free speech issues on the internet were elaborated. At the discussion session, the special regulations of schools were argued.

"Free speech in other countries" and "Free speech issues in the school setting" were discussion forum topics of this week in the online environment of the course. In the "recommended links" section, the researcher proposed three articles "*Definition of Hate Speech* (Parillo, 2008)", "*Hate Speech* (Parekh, 2006)" and a reference book (Georgescu, 2016). It was a 216-page book. The researcher proposed this book for a reference for the students' professional lives. In particular, she underlined the subsection, namely "*Guide to Human Rights for Internet Users*" to be read.

In the extended lecture notes, the terms *speech*, *freedom of speech*, *hate speech*, *symbolic speech*, and *censorship* were defined. The etymologic background of the phrase "free speech" was explained. The researcher demonstrated some examples of free speech from News sites. The notes included the constitutional elements of the US, EU, and Turkey as well. A discussion about censorship and the internet related issues were explained.

---

[e] https://constitutioncenter.org/interactive-constitution/amendments/amendment-i
https://www.history.com/topics/freedom-of-speech

[f] https://www.tbmm.gov.tr/anayasa/anayasa82.htm

[g] https://www.echr.coe.int/Documents/Convention_ENG.pdf

[h] https://www.policyed.org/intellections/limitsoffreespeech

The dictionaries; Merriam-Webster, Oxford Dictionary, Britannica, Encyclopedia of Social problems, and Legal Dictionary were the sources of information for the definitions. The internet resources of; "History.com, Constitution Center, Equality and Human Rights Commission, No Hate Speech Movement" and the e-zine articles from "NY Daily News, The Association for Supervision and Curriculum Development (ASCD), and Education Policy" were the resource of information used in the preparation of the lecture notes.

4.1.3.4.9. The Ninth Session – Addiction

In the ninth session, *addiction* was the major topic. The following subtopics were covered in the lecture; (i) *the stages of addiction,* (ii) *definition and types of computer addiction,* (iii) *addicted behaviors,* (iv) *results of addiction,* (v) *game industry and addiction,* and (vi) *avoidance* (*from addiction*) methods.

In the former semester, addiction was briefly introduced in the fourteenth week. Compared to the former implementation, the researcher defined and described addiction in more detail this semester.

The realized program of this week was completely different from the syllabus. Addiction was planned to be covered in the seventh week this semester, as the second part of the lecture. As it was explained before, it is postponed to this week. The topics which planned to be covered this week were covered in the seventh week. A summary of the course, the differences between the official and realized program, and description and the explanation of the differences are presented in Table 4.24.

Table 4.24. *Change in the Course Curriculum, the Ninth Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 9: April 10	Threats, Security issues on Digital Identities • Precautions on SNSs, Fake Profiles • Hoax and Clickbait	Addiction • Cyber-addiction • Signs and Results of Addiction • Avoidance from addiction
	Description	**Rationale**
	Fraudulent content was explained in the sixth week of the semester.	It was explained in a part of "Safety Issues of the SNS

The lecture started with the definition of *addiction*. Then, *stages* and *types of addiction* were explained. *Nomophobia*, a special type of mobile addiction, *game addiction* and how *the game industry* encourages addiction were described. The *effects of addiction* on the individuals were listed. The lecture session has ended with brief information about *avoidance strategies from computer addiction*. At the discussion session students' observed or lived experiences about addiction were discussed.

In the extended lecture notes, the terms covered in the lecture were elaborated in detail. Different sources of information were used in the design of the course this week. The dictionaries Merriam-Webster and Medicine Net Glossary provided information for definitions. The internet resources; Addiction.com, Medicine.net, American Addiction Centers, Online Psychology Degrees were used for the contents of the lecture and lecture notes.

4.1.3.4.10. The Tenth Session – The Second Mid-Term Exam

The exam consisted of 21 multiple choice test questions. Twenty questions of the test were 5 points, with four answer choices, one of which was correct. The 21st question was the bonus question with 10 points value with five answer choices. Total points they can get from the exam was out 110. Of the 21 registered students, 17 students took the mid-term exam, and 3 took the make-up exam. The makeup exam was similar to that of mid-term without bonus question.

The test questions were related to cybersafety issues. Definitions of or examples related to the following topics were asked in test questions; privacy, PII, unique identifier, NORA, clickbait and HOAX, safe and responsible use of SNSs, sharenting, oversharing, cyberbullying, freedom of speech, symbolic speech, addiction, computer addiction, mobile addiction.

As a bonus question, four people, Galileo Galilei, Pythagoras, Hypatia, and Farkhunda were asked to the students. Their common characteristics were that they have been subjected to violence or killed because they expressed their ideas. The question was "Which of the following persons have been arrested or subjected to violence or killed because they expressed ideas?" The correct answer was the fifth choice "*All of the above*." The correct answer rate for the bonus question was 71%.

4.1.3.4.11. The Eleventh Session – Principle issues on Information Security

In the eleventh session of the second implementation, cybersecurity issues were introduced to the students. Definitions of *information*, *information security*, and *information assets* were presented. Afterward, the terms *CIA Triad*, *information security truisms*, *vulnerability*, *exploit*, *threat*, *impact*, and *risk* were defined in detail. Later, *threat types* and *human threats* were clarified.

In contrast to the current semester, the information security related topics were covered at the beginning of the semester in former implementation. Particularly; the term *information security* was introduced in the third week of the first implementation. Due to the reasons stated in the summary of section 4.1.3.2, these group of topics were located on the last four weeks of the current implementation.

The contents of the lecture were almost the same as it was in the syllabus. The only difference was the inclusion of a detailed explanation of threat types in information security. Brief information about the session is presented in Table 4.25.

Table 4.25. *Change in the Course Curriculum, the Eleventh Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 11: April 24	Principle issues on information security • Major terms and CIA Triad • Security truisms • Risks and attack types • Hacker Types	Threat types were included
	Description	**Rationale**
	The examples were chosen to be from the non-computer domain.	Giving examples from the students' daily routine lessens their concerns about the course.

Before beginning the lecture, the researcher asked the students about some basic information security issues. How often they change their user passwords and whether or not they use antivirus software were the two examples questioned in the session.

The lecture started with the definition and explanation of *information security* and related terms. The main objective of information security is to prevent *Confidentiality*, *Integrity*, and *Availability* (*CIA Triad*) of information.

Throughout the lecture, the researcher gave non-computer examples of security truisms, vulnerability, risk, and threats. The majority of non-computer examples were related to security issues about banks or security measures taken in markets. The common threats on *Automatic Teller Machines* (*ATM*), security breaches of *Point of Sale* (*POS*) devices, security levels of banks were some of the presented examples.

Several sources were used for this session. The contents of this lecture are arranged with the first and fifth chapters of "*Computer Security Literacy* (Jacobson & Idziorek, 2016)" and the second chapter of "*Information security: principles and practices* (Merkow & Breithaupt, 2014)."

In addition to these sources, the examples and detailed explanations of the terms were obtained from the following sources (Greene, 2004; Whitman & Mattord, 2012). The lecture included *threat types of information security* (Easttom, 2016; Smith, 2016) and *hardware security and safety in schools* from the online sources and books (Wikibooks, 2016) and (Szuba, 1998).

In the online environment of the course, the researcher asked the students to give different information security incidents and appropriate protection measures. The incidents might either be a part of their own experiences or their imaginary scenarios.

In the recommended resources section, different resources presented to the students. Definitions of major terms in a part of ISO27000 series (ISO, 2018); the first and fifth chapters of "*Computer Security Literacy* (Jacobson & Idziorek, 2016) were provided as an information source. In the extended lecture notes, the terms and examples were presented in more detail. These books were the main sources of information.

4.1.3.4.12. The Twelfth Session – End users and Information Assets

In the twelfth session of the second implementation, *end users*, *information assets* and *precautions on assets* were explained. *Phishing* and *fake notification* were

clarified. The *security issues about mobile devices* were included. The topics of this week were covered in the fourth session in the previous semester.

The realized program of the course was slightly different from the syllabus. Originally in the fourteenth week, mobile related issues moved to the current week's program. The end users' role in the security of information assets were highlighted. A summary of the course week is presented in Table 4.26.

Table 4.26. *Change in the Course Curriculum, the Twelfth Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 12 May 8	Information assets • Digital assets • Print-based information assets • Hardware assets, Hardware Security tips • Physical Security • Virus protection and Backing up and restoring • Soft assets	• Asset, Asset types • End users, definitions and responsibilities • Asset types for end users • Security tips for all types • Security tips for Mobile Users • Security of Digital identities ○ Phishing, Fake Notifications
	Description	**Rationale**
	Information about Mobile security was included.	The protection measures for mobile users were similar to hardware protection methods. The device specific points were highlighted.

The lecture started with the definition and descriptions of *information assets*, *asset types*, and *end users*. *End users' responsibilities* as a measure of information security were clarified. Protection strategies of information assets were listed. As the protection of digital assets, *phishing* is defined and described in detail. In the discussion session; firstly, online phishing activity was done (Phishing.org, 2018). Then, several information security incidents the students observed or experienced were discussed in the classroom.

In the online environment of the course, a guideline for end users "*End User Computer Security Responsibilities* (Elekwachi, 2002)" and an e-book "*Essential Computer Security* (Bradley & Carvey, 2006)" were recommended to the students. In the extended lecture notes, the terms and examples were presented in more detail. The

security tips (Elekwachi, 2002) for different kinds of information assets were provided for the students. The ISO 27000 glossary (Calder & Watkins, 2010) was the main source of information for defining the terms. The online resources of Computer Security Resource Center (csrc.nist.gov), The European Union Agency for Network and Information Security (ENISA) (https://www.enisa.europa.eu/), System Administration, Networking, and Security Institute (SANS) (sans.org), Global Information Assurance Certification (giac.org) and the e-books of (Elekwachi, 2002)" and (Bradley & Carvey, 2006) were the resource of the lecture notes.

4.1.3.4.13. The Thirteenth Session – Identity Security and Safety

In the thirteenth session, the topics *digital identity*, *password* and *authentication types*, *trusted* and *untrusted networks*, and *malware* were covered. The possible threats of untrusted public local area networks result in a security breach in the use of mobile devices. In the previous semester, the topics of the current week were covered in the fifth and sixth sessions.

Table 4.27. *Change in the Course Curriculum, the Thirteenth Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 13 May 15	Digital Identity theft • Phishing • Passwords protecting • Social Engineering	Digital Identity • Definition, protection measures Password Management • Requirements of password • Multi-level authentication Threats of Untrusted local area networks Malware (Definition and types)
	Description	**Rationale**
	Phishing was explained in the previous week.	Protection of digital identities was introduced in the previous session; this week it was explained in more detail.
	The phrase "Untrusted local area networks" was introduced.	Untrusted local area networks are important threats in the scope of mobile communication.

In the discussion session, students' password management strategies were discussed. Furthermore, the risks and benefits of these strategies were discussed in the

class. The responses are summarized in Chapter 4. In the extended lecture notes, the terms and examples were presented in more detail. The books mentioned in the previous section is used as a source of information and recommended to the students. A summary of the course week is presented in Table 4.27.

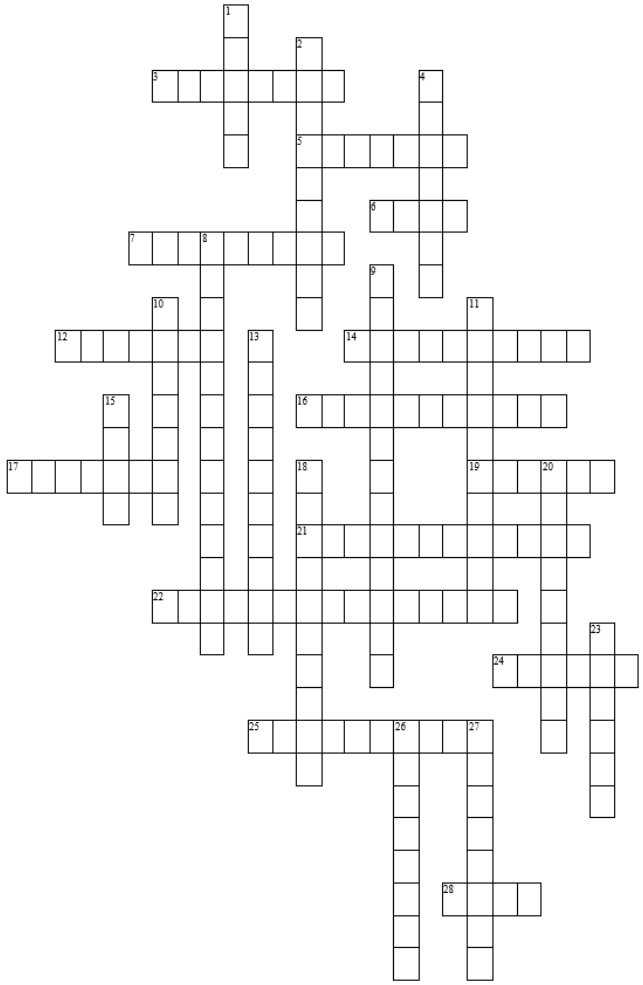
4.1.3.4.14. The Fourteenth Session – Overall Summary

In the last session of the second implementation, all the topics covered in this semester were briefly summarized. The syllabus and the realized program were different. Mobile Security issues, supposed to be covered in the current week, were introduced to the students in previous sessions. A summary of the course week is presented in Table 4.28.

Table 4.28. *Change in the Course Curriculum, the Fourteenth Week of the Second Implementation*

	Syllabus	**Realized Program**
Week 14 May 22	Security issues on Mobile devices • Critical issues on the use of Mobile devices • Trusted applications • Permissions of applications	The overall summary is presented
	Description	**Rationale**
	Security issues of Mobile Devices were explained in 12th and 13th weeks.	In the first implementation, mobile security topics seem to be a repetition of the previous topics.
	Q&A session was conducted.	Before the final exam, in the last session of the semester, guiding misunderstood topics was beneficial for the attended students.

The researcher realized that the students tried to study the course topics by memorizing the contents, which in turn further confuses themselves. The overall semester brief was beneficial to clear some of the misconceptions. A crossword puzzle with 28 course related terms was also prepared and distributed to the students in the class. It was uploaded to the online environment of the course. The puzzle is presented in Figure 4.9.



Across

3. A form of fraud in which an attacker masquerades as a reputable entity or person in email or other communication channels

5. An unimplemented method or algorithm that is able to take advantage of a vulnerability in a computer system

6. A humorous or malicious deception

7. Something designed to make readers want to click on a hyperlink especially when the link leads to content of dubious value or interest

12. Malicious software that observes user's information (passwords, etc.) and actions and then sends that information to a cybercriminal

14. Intentionally or unintentionally acquiring and using someone else's ideas and opinions and presenting them as if one's own without making a reference to or citing the source

16. An attack on a Bluetooth enabled device (usually a mobile phone) in which an attacker sends an unauthorized message to the device

17. The person that a software program or hardware device is designed for.

19. Measure of potential consequences if the computer system or the confidentiality of information was compromised as the result of a security breach

21. Property of being accessible and usable on demand by an authorized entity

22. Property that information is not made available or disclosed to unauthorized individuals, entities, or processes

24. Potential cause of an unwanted incident, which can result in harm to a system or organization

25. The suppression or prohibition of any parts of books, films, news, etc. that are considered obscene, politically unacceptable, or a threat to security

28. An autonomous and malicious software program propagating among computer networks

Down

1. Anything that has value to the organization, its business operations and their continuity, including Information resources that support the organization's mission

2. Property of accuracy and completeness

4. the ability to control information about oneself

8. The act of using the Internet, cell phones, video games, or other technology gadgets to send, text, or post images intended to hurt or embarrass another person.

9. A weakness in some aspect of a computer system that can be used to compromise a system during an attack

10. All malicious software, including viruses, Trojan horses, and worms

11. A person who targets computer systems or websites with the motivation of making ideological, political, or religious statements

13. The fear of being without a mobile device, or beyond mobile phone contact

15. Measure of the criticality of a situation--the likelihood of something being attacked

18. A specific type of over-sharing, which represents the habitual use of social media to share news, images, etc. of one's children

20. A software that detects and cleans computer viruses

23. A person gaining unauthorized access to computer networks, systems, or data who breaks into computer systems

26. Listening in to information that is transmitted over the air including verbal conversations with an objective of learning private information

27. A string of characters that allows access to a computer, interface, or system.

Figure 4.9. Information Security Puzzle

4.1.3.4.15. The Final Exam of the Second Implementation

The final exam consisted of 26 multiple choice test questions. Each question was 4 points. Total points they can get from the exam was 104. The average score was 73.6. The highest grade among the students was 92. Seven students got 80 and higher grades.

In the final exam, all objectives of the course were tested out. The exam included the major topics of the cyberethics and cybersafety and topics of the last five weeks, namely information security, end users and information assets, mobile security issues, identity security, and safety.

4.1.3.5. Summary of the Second Implementation

Throughout the semester, the researcher utilized the resources which were used in the former semester and enhanced the content with additional current information sources. The number of forum discussions is increased. With the inclusion of extended reading notes, the researcher developed a detailed course content.

To summarize; the extended lecture notes were prepared. The content sequence has been redesigned for the second implementation. There have been minor arrangements about the subtopics for each week. These minor arrangements are presented in the corresponding subsection. The term based summary of the differences and weekly session summaries are presented in Appendices J and K respectively. The visual representation of the research phase is presented in Figure 4.10.

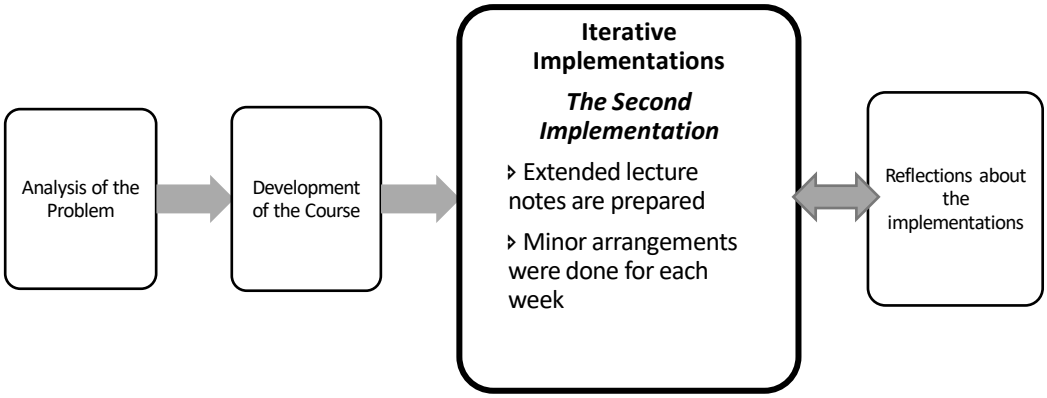


Figure 4.10. Design-Based Representation of the Study – Iterative Implementations: Phase 2

4.2. The Design Issues about the Content, Learners, and Instruction

The theme “design issues” was an important theme that emerged from the qualitative analysis. During the needs analysis phase, the potential topics to be taught in the course were determined. During the development and the implementations of the course, every single detail of instruction is regarded as a design issue.

The data sources of this theme were the analysis phase findings, the interviews, both with the experts and the students, the researcher’s designer reflections, and field notes. Analyzing the qualitative data of the study, several design related issues emerged. They are grouped as the content, learner, and instruction related design issues.

4.2.1. Content Related Design Issues

The multidisciplinary nature of the course has affected the determination of the subtopics. Content pool and the content sequence were critical points of concern. How they were designed and developed was explained in the previous section. In this section, the critical content related issues encountered during the study were explained.

4.2.1.1. Needs Analysis Phase – Creation of the Content Pool

The researcher conducted several semi-structured interviews with the experts from Computer Center, Computer coordinators in Faculty of Education, Faculty members in CEIT, educational sciences, philosophy and psychology departments. The researcher also reviewed the Computer Center Helpdesk incidences. The needs analysis study was not limited to the technical incidences in the university. The information security issues in the literature were also reviewed. The detailed process of needs analysis is explained in Section 4.1.1. Having all reviews and interviews done, the content pool was prepared. As a result of these preliminary analyses, the initial content pool with raw content has emerged and presented in Table 4.29.

Table 4.29. *Content Pool of the Course: Pre-Implementation Phase*

Cybersecurity	Virus protection, Peer to peer network use, mobile security, untrusted networks, password protection, and hardware protection from physical threats
Cybersafety	Cyberbullying, preservation of digital identity, sharenting, oversharing, game addiction, social engineering
Cyberethics	Netiquette principals in online communication, digital reputation, freedom of speech and its limitations, digital rights, censorship, intellectual property, cyber plagiarism

4.2.1.2. The Sources Used in the Implementations

The contents covered in each lecture were explained in detail in section 4.1.3.2. This section includes the summary of the field notes, students' participation and contribution details both in lecture sessions and the online environment of the course, and exam results.

The contents of the information security related lectures are adopted and summarized from the books; *The Basics of Digital Privacy* (Cherry, 2014), *Computer Security Literacy* (Jacobson & Idziorek, 2016), *Elementary Information Security* (Richard E Smith, 2015), *Information Security in Education* (Wikibooks, 2016) and *Safeguarding Your Technology* (Szuba, 1998). The Internet resources of the topics were TechTarget and Dictionary of Merriam Webster (for definitions).

The cyberethics related topics, such as freedom of speech, copyright, and legal issues on the internet included terms of the law. The lecture about the freedom of speech included the definition and constitutional statements such as Article 26 in the Turkish constitution or European Union (EU) Statements, and the First Amendment of the US constitution.

The researcher provided recommended links in the online environment of the course. The reading materials were either available in the library of the university or provided as pdf® document by the researcher. The lecture documents were selected in line with fair use principles of the copyright holders.

4.2.1.2.1. Change in the Course Outline in the First Implementation

The syllabus has changed during the semester in the first implementation. In the first implementation, the lecture contents were prepared during the semester. In the first few weeks of the semester, while covering the information security related topics, some of the students' appeared to be concerned about the technical level and difficulty of the topics; and they communicated these concerns to the researcher. At this point, it was not easy to make a radical change in the course outline, but the researcher made a major change in the course syllabus and increased the time allocated for information security part of the course. By doing so, she explained information security topics in detail with anecdotal examples. It affected the period of other main topics. As a result, in the first implementation, addiction, cyberbullying and free speech topics were given in one lecture session.

During the semester, information security took seven weeks one of which included a general review. After the first exam, cyberethics and cybersafety related concepts were introduced. However, in this case, through the end of the semester, because of time limitations, some of the ethical concepts were presented briefly, such as digital equity or censorship. During the semester, two midterms were held in two separate weeks at lecture hours. The contents of those weeks were distributed to previous or successive weeks.

The syllabus of the first implementation is presented in Appendix F. Difference between the official and realized content sequence in the first implementation are presented in Appendix G. The brief lecture summaries of the first implementation are presented in Appendix H.

4.2.1.2.2. The Reflections and the Major Issues – Second Implementation

According to the findings and suggestions obtained in the first implementation, the course syllabus was rearranged. Each week, the lecture notes were also presented to the students besides the lecture presentation. The course contents were grouped into three main topics which were Cyberethics, Cybersafety, and Cybersecurity. The student evaluation policy remained the same, two midterms, one final and participation.

The content sequence has not been changed during the semester in the second implementation. The syllabus of the second implementation is presented in Appendix I. Some minor changes in the syllabus were made during the implementation. Realized content sequence and difference between the syllabus and realized lecture programs in the second implementation are presented in Appendix J. The brief lecture summaries are presented in Appendix K.

The course materials, presentations, reading assignments have been prepared in the previous implementation. In the second implementation of the course, the topics addiction and freedom of speech were extended. They were briefly explained in the first implementation. During the design of the course materials, the prepared documents were used and rearranged. New forum discussion topics were included. Extended lecture notes were prepared. The content details of extended lecture notes were explained in Section 4.1.3.4.

The other departments in the Faculty of Education did not enroll in the second implementation. One of the major reasons for this situation was the weekly schedule of the course. According to the schedule, the lecture hours were on Tuesdays, 12:40 – 15:30. The instructor stated that the must courses were generally scheduled on the first half of the week, and the students may not be able to enroll in the course.

4.2.1.3. The Syllabus Change between the First and Second Implementations

The design of the content sequence of two implementations is explained in detail in the previous sections. The researcher included various materials in lecture presentations. The contents were explained briefly through lecture presentations, and the controversial issues were discussed in the discussion session that week. The researcher also provided additional reading materials and video links for the students, so that they would be able to understand the topics better.

The course outline in the second implementation was redesigned according to the findings of the first implementation. The new outline is presented in Appendix I. The 14 weeks of the semester was evenly divided into three parts to describe the cyberethics, cybersafety and cybersecurity issues in detail. During the semester, in the fifth and the tenth week, two midterm examinations were held instead of a lecture.

One of the major differences between the first and second implementation was that the lectures related to cybersecurity were given at the end of the semester in the second implementation. The two participants who were enrolled in the first implementation were also suggested the content sequence would be rearranged so that the information security terms would have been given after ethics and safety parts were given.

The researcher presented the new content sequence to some of the students of the first implementation for their opinions. In general, they found it meaningful and beneficial. One participant (M105) describes this change as follows:

> First the general concepts (*ethics*) are given, the students have an idea about what is right or wrong in a cyber world, then they introduce the potential threats (*safety*), and after presenting these preliminary issues about cyber world throughout the semester, how to guard against these threats (*security*) are being explained. It is a better content sequence (M105).
>
> *Önce genel bilgiler (etik) veriliyor, öğrenciler ne doğru ne yanlıştır öğrendikten sonra yani mantığı oturttuktan sonra buna karşı olası tehdit (cybersafety) ne. Bu konuda temel bazı bilgileri verdikten sonra ben buna karşı nasıl savunabilirim mantığı daha iyi. Tehdidi bilmeden de savunamazsınız. Bu daha iyi bir konu sıralaması olmuş (M105).*

In the majority of the semester, the lecture contents were the extension of the previous implementation. As in the previous implementation, specific details for pre-service teachers were also included in the lecture and discussion sessions. Due to time limitation in the first implementation, the researcher was unable to explain the two topics which are addiction and freedom of speech. The contents for these topics were extensively developed in the second implementation.

Decisions of subtopics in some sessions were a matter of concern. The main topics Copyright and Addiction were two underlined topics by some interviewees. Intellectual Property and related concepts, such as copyright and DMCA found to be

complicated and confusing in the first implementation. The reason was that there was another topic covered that week. In the second implementation, it was simplified and purified for the pre-service teachers' needs. Similarly, the interviewees of the second implementation stated that there were repetitions in addiction subtopics.

In the second implementation, due to the radical outline change, the period of some topics was changed. On the other hand, the detailed subtopic breakdown remained the same for some of the main topics. However, there were differences between the first implementation and the second implementation. The topics given differently for the second implementation are listed in Appendix 0. The term based weekly outline differences between the two implementations is demonstrated in Appendix N.

4.2.1.4. Confusing Topics

The researcher realized that some topics covered in the same lecture hour were confused by the students. In the interviews, two students stated that they confused the *Law 5651* and *ISO 27000*. The students' confusion about Internet Law and Information Security Standards was realized in the first exam of the first implementation. About 43% of the students in the first implementation have answered the question is asking *the series number of information security standards* wrong. For this reason, the researcher, in the second implementation, explained them in different sessions.

Similarly, three students mentioned they did not understand the difference between the terms *hoax* and *clickbait* at first and added that they understood in the exam, which the difference was asked. Hoax and clickbait, both are the names of certain types of fraudulent content. They are different in a way that while clickbait refers to the exaggerated title of any content, hoax refers to deceptive content. Shortly while clickbait is a name of deceptive titles, hoax stands for fake contents. It was highlighted several times both in the lectures and in the discussion forums. The difference was asked in the exams both in the first and the second implementation. Correct answer rate was 93% and 88% in the first and second implementations respectively.

4.2.1.5. Suggestions from the Students

The CEIT students said that the technical level of the course was lower than their expectation. The non-CEIT students, on the contrary, found the technical level of the course, particularly cybersecurity-related topics were difficult to understand. They suggested these terms to be simplified. These oppositely different responses indicate that; the new terminology related to cybersecurity would be explained differently. Another suggestion from the students was about the examples. Although the majority of the students liked the variety of examples, they also added that the number of examples would be increased.

The students' other suggestions include; increasing in the number of examples, shortening the reading materials, and including audio-visual materials for the lectures. To summarize, content related issues about the course include the content pool and the content sequence, being aware of the confusing topics, employing different types of instructional materials.

4.2.2. Learner Related Design Issues

The potential learners of this course were the pre-service teachers. The students were from different majors and in their different years. These differences affected the implementations. These critical issues were presented in this section.

4.2.2.1. Learners' Prior Knowledge

The students were, in general, dense users of SNSs and were familiar with ethical issues, such as free speech or censorship. The enrollees of this course were from different departments of faculty of education. For this reason, their prior knowledge and their approach to several parts of the course were different. The CEIT students mentioned that they already knew most of the topics before. Their prior computer-related knowledge was different from the other departments. However, as it was mentioned in the Section 4.4.1, *Newly Learned Topics*, most of the students, including CEIT students, mentioned that even though they knew some of the topics before, they had chance to learn that topic in detail.

The students were asked whether they heard about any of the topics covered in the course before. Majority of the students declared they knew some of the topics, among 23 interviewees only four students stated that they knew nothing but have learned almost all the topics for the first time in this course. However, after an in-depth interview, three of them referred to their prior knowledge about some of the topics.

According to their statements, the most familiar topic was cybersafety issues in social media, particularly fraudulent content. Thirteen out of 23 students declared that they were familiar with privacy issues or fraudulent content in social media. Besides, some of the students demonstrate their concern about K12 students, who are actively involved in online activities and more vulnerable compared to adults. The interviewees highlighted that teenagers were very active, cyberbullying was a major concern among them, and on the other hand, some of the parents were not aware of such issues.

Cybersecurity topic was the least familiar to the students. Only five of 23 students stated that they knew password security issues. Three students stated the other topics on cybersecurity, such as information assets, hardware, and mobile security as familiar topics. Security certificates of the web sites was an unknown topic for the students as expected. Only one participant, who worked as an intern in the Computer Center of the university, stated that she knew before since she has worked about web sites' security certification.

The source of their prior knowledge was based on a variety of sources. Their special interest, having experienced some of the topics, such as cyberbullying, or hate speech or recalling some of the topics from the previous courses were some of these sources. Some CEIT students declared they have graduated from vocational high school and they were well informed about fundamental issues on information security. However, most of them emphasized that they were familiar only with the names of the terms. They continued that they had a chance to cover most of the topics in detail, such as clickbait or phishing in this course.

To summarize, safety issues of SNSs, such as fraudulent content or SNS addiction were the topics with which the students said they were familiar. The students were familiar with SNSs and fraudulent contents. According to their responses, the

primary source of this familiarity is their daily life experiences or observations. CEIT students acknowledge the courses they took before and the vocational high schools they have graduated.

4.2.2.2. CEIT and Non-CEIT Students

The responses from CEIT students and non-CEIT students were oppositely different. CEIT students responded that the course contents were easy and they expected the cybersecurity topics to be explained in more technical detail. On the other hand, the non-CEIT students thought that cybersecurity topics in the course were given too detailed. The verbal nature of the course seemed easy for FLE students, while CEIT and MSE students felt difficulty. Few of the responses are given below

> We, the CEIT students expected this (*technical level of the course*) to be given in more detail. We expected the (*information security*) terminology to be covered. However, the details are not covered since the students from the faculty of education took the course as well; I believe (M106).

> *Biz BÖTEciler olarak daha detaylı bekledik. Terminolojiye girilmesini bekledik. Ama eğitim öğrencileri ile alınca sanırım teknik detaylara pek girilmedi (M106).*

> If you want to heighten awareness of students more, the content could be somewhat more technical. For example, I am aware that your knowledge is deeper; for example, a major network attack has been experienced; we would like to have more information about this (M115).

> *Eğer öğrencileri daha fazla bilinçlendirmek istiyorsanız eğer, içerik biraz daha teknik olabilir. Mesela sizin bilginizin daha fazla olduğunun farkındayım ben, mesela bir büyük ağ saldırısı olmuş, biz bu konuda daha detaylı bilgi almak isterdik (M115).*

> Since we enrolled this course with the students of the Faculty of Education, it could be at this level. We, as CEIT students, expected the security topics would be in more detail (M205)...
>
> *Eğitim Fakultesiyle beraber alındığı için anca bu kadar olabilirdi. Biz BÖTEci olarak security konularının biraz daha detaylı olmasını isterdik (M205)…*

On the other hand, the students from other departments of faculty of education conversely claimed that the terms were confusing and they are needed to be simplified. They claim that the information security topics required prior knowledge about computer systems. Two examples are given below.

> I had a hard time while I was studying security issues. Had a hard time studying attack types, integrity, and definitions. I know how to do but had a hard time while studying (M105).
>
> *"Security issues"ları çalışırken zorlanmıştım. saldırı tipleri, bilgi bütünlüğü konusunu, tanımları çalışırken zorlanmıştım. Ben biliyorum nasıl yapacağımı, ama anlatırken zorlanıyordum (M105).*
>
> I had difficulty to comprehend the terms. We could comprehend the general things, password, phishing, etc. You provided plenty of examples. However, what is an attack, what is zero attack, we had great difficulty in comprehending them (M110).
>
> *Terimleri algılamakta zorlandım. Genel şeyleri algılayabildik. Password phishing… falan… Phishing falan anladık. Çok örnek de vermiştiniz. Ama atak nedir zero atak nedir onları algılamakta çok zorlandık (M110).*

CEIT curriculum provides the students programming, database, operating system, and several software skills and raises their computer literacy. On the other hand, the verbal part of the course, such as ethics and safety issues were not explicitly provided in a course in their curriculum. Some of the cybersecurity topics, which CEIT

students think that they already knew, are also included among their newly learned topics.

4.2.2.3. Unwillingness to Reading

Another important characteristic of the students is that they do not prefer reading. Some weeks, the researcher announced a reading material for the content of that week. The purpose of giving a reading assignment was that the topics would be explained in detail. One of the students stated that they would have read if readings would have been shorter. In the first implementation, the course schedule was on Fridays. Each Monday, the researcher sent the weekly recommended reading list on the course website. The researcher designed the lectures in the form of PowerPoint® presentations.

In some cases, she asked questions about their opinions on corresponding topics. The students could have easily answered such questions if they had read the reading materials. However, the students declared that they did not read; they did not prefer reading or did not have time to read. The recommended links included not only the reading documents but also the video links. Many students admitted not watching the videos either. Therefore, the weak reading habit was not the only reason for not following the links. According to the interviews, it is believed that one of the major reasons for not following the links is that while students log in to the learning management system of the university, they forgot to log to the website of this course.

The method of instruction and preferences would be designed according to the feedback and participation of the students. The two major negative feedback of the students were related to technical wording of the course and existence of reading materials. Another characteristic of the students, the researcher realized was that they did not prefer to participate in forum discussions.

In the second implementation, the students' participation was better compared to the first one. There were several occasions when spontaneous debates occurred in the class. One of them was about the academic dishonesty types. While presenting the academic-dishonesty types, the researcher gave an example for bribery as selling the registered courses in the registration period. The enrolled students stated they did not

sell any registered course, but have been victims of such dishonesty type. Then, they complained about the registration issues and difficulties of registration to "popular" courses. Some of them justified this with the difficulty of the registration period. Another topic which the students reacted was "self-plagiarism." It was noticed that self-plagiarism was not understood and is a common threat to academic integrity at the undergraduate level. Some of the students recall their low graded homework. Their objection was based on the premise that both works were their intellectual property and they question why they could not use the same work for different homework.

4.2.2.4. Students' In-class Participations in Both Implementations

Throughout the semester, the students were able to ask questions, reply to the questions during the lectures. Each lecturing session was starting with reminding the prior contents, giving brief information about the contents of the current lecture. The instructor generally asked whether they know anything about the current subject, or correlating that week's topic with current hot news.

4.2.2.4.1. The First Implementation

Forty students enrolled in the course. The average attendance rate was 76%. During the registration period, the students refrained from taking the course because the course has been given for the first time, and the students worried about the difficulty of the course. The reason for the students' concern was about prejudice to a computer-related course and the anxiety about the grading of a course which was not given before. The students took this course as an elective course. In the first session of the course, and during the registration period, some of the students stated their computer related concerns. One of the major questions they asked was whether there would be computer-related homework or not.

In the *first* session, after talking about the general course policy and lecturing part; the researcher asked whether or not the students have at least one SNS account. All students stated they had an account on at least one SNS. Majority of the students had Instagram® and Facebook® accounts.

In the *second* session, during the introduction to the topic "information security," the researcher encountered that the students had a false belief that their assets

were not very important. They did not care about the threat of identity theft. In this regard, the instructor stated that the issue of identity theft is not about the importance of their digital assets. Cybercrime is often performed on stolen digital identities.

On the *third* session of the first implementation, the topics related to information security were elaborated. On the discussion session, the students shared their password management strategies. Most of the students stated that they would rarely change their passwords. They also added that they increased the privacy settings of their SNSs.

After the lecture session, a group of students complained about the technical level of the course was rather high to comprehend. They also claimed that the topics covered in that session were perceived to be very difficult to understand.

During the *fifth* lecture session, the topic "digital identity" was explained, the researcher asked whether it was possible to create a password that no one can break. Some students responded that it was not possible to create such a password and recalled the security fact "absolute security does not exist." It demonstrates that the students were able to link prior knowledge to present contents.

In the *sixth* session, the topic "Mobile Security" was explained. During both the lecture and discussion hour, the students demonstrated high participation in this lecture. It was probably a natural result of the high usage of mobile devices among students. In the lecture, the security issues about the mobile application, in particular, the permissions that they mandate the users were argued. One of the students stated that she installed an exercise tracking application and that application asked for permission to use contact list.

In the discussion session of the *seventh* week, the students shared their different information security incidents. They mentioned that they had been more suspicious on the Internet.

In the discussion session of the *ninth* session, the students' experiences on different ethical concerns or decisions were discussed. One of the students reminded a video taken by a teacher in a classroom and spread in social media, which was about a little girl was complaining about her socioeconomic situation. There were several

ethical problems in that video. It was a serious ethical violation to publish video recordings of students on the Internet. The ethical issues and the existing regulations were discussed in the classroom.

The recording or taking photo of the students is a violation of "Do not Track Statement." One of the students gave an example about Sweden; her experience once had during Erasmus, that she could not take a photo of an activity. According to EU regulations, unless the parents of the children explicitly approve audiovisual recording and taking a photo, one cannot take video or picture of the children.

At the beginning of the *thirteenth-week* lecture, students' social media behaviors were questioned. Some of the students contributed by explaining their SNS usage preferences, how often and for what purposes they use. The students highlighted that; they increased their account's security levels. They stated that they were not disclosing much of their information.

4.2.2.4.2. The Second Implementation

In the second implementation, 21 students enrolled in the course. The average attendance was 71%. As it was in the previous semester, the students' concern about computer related course continued. Contrary to the first implementation, some of the new enrollees were advised by the students of the first implementation.

At the discussion session of the *first week*, students' expectations from and concerns about the course were asked. Similar to the first implementation, students in this semester has come to class with their concerns regarding their low level of computer literacy and worried about whether or not there were coding or similar activities. The instructor's response was that; there were no coding activities and highlighted that participating both in in-class activities and online forum discussions were required. Students' expectations from the course were different. Being an elective course, besides a good grade expectation, they were also eager to learn cybersafety issues in more detail. For example, privacy issues in social media and how to deal with a cyberbullying incidence or game addiction were the common topics the students were curious about.

In *the second week*, during the discussion session, legal, ethical and moral concepts were compared. Contradicting or supporting examples were asked. The first example from the students was about child marriage. It is illegal, unethical, but accepted as moral in rural parts of this country. The Wikipedia ban was also discussed in the classroom. The banning procedure depends on the law 5651 and legal. The lecturer asked whether it is ethical or not. Does it violate the information access and free speech rights? A student highlighted that the being legal of banning was also unethical. Another view about Wikipedia ban was that the reason for banning was not apparent.

In *the third week* of the course, while explaining academic dishonesty types by examples and lived experiences, students' contribution enriched the contents. For example; while presenting the academic dishonesty types, the researcher, as the teaching assistant of the course, gave an example for bribery as selling the registered courses in the registration period. The students complained about the registration issues and difficulties of registration to "popular" courses.

Another topic which the students reacted was "*self-plagiarism*." It was noticed that self-plagiarism was not understood and is a common threat to academic integrity at the undergraduate level. The students also added some students' digital cheating strategies in order to bypass plagiarism detection tools.

In the discussion session, the difficulty level of the make-up exams was questioned. Some of the students advocated that the make-up exams could be more difficult compared to the mid-term exam, and it was not regarded as an ethical issue because the student might have more time to study.

In the *fourth week* of the second implementation; intellectual property related issues were explained. The students' contribution to the lecture was about patent and trademark issues. In particular, medicine patents or trademark violations were exemplified.

In the *sixth week* of the semester, cybersafety issues were introduced. Before the lecturing session, the researcher asked what they know about privacy. They contributed to the legal perspective of their privacy. In other words, governmental

authorities' right to obtain details of private communication was argued from an ethical perspective. One of the students asked whether the authorities could be able to get their private communications in detail. A debate occurred with one side supported the legal responsibilities of the authorities and the opposing side who declared that it was a violation of private life. During the lecture, when sharenting issues were explained, the students told about their parents' behaviors as an example of sharenting. They also questioned that, whether or not a teachers' sharing their students' PII was a sharenting attitude. In the discussion session, the researcher asked the students whether they have any social media account. Proper and improper SNS behaviors were discussed. Almost all of them have a Facebook® account. Although some of the students declared they were not using actively, it was still one of the most frequently used social media tools.

In the *seventh session* of the second implementation two main topics; teachers' SNS use and cyberbullying were lectured. At the beginning of the lecture session, the researcher asked about teachers' social media interaction with their students, whether it was a right or wrong habit. Almost all students highlighted that it might have some negative effect on the students. They also expressed the teachers' potential privacy problems in case of an interaction with students. In the second part of the session, when cyberbullying related issues explaining, some of the students participated in the lecture and shared their lived or observed experiences about bullying or cyberbullying. During the lecture, the lack of policy in schools aiming at protecting bullying behavior was argued.

At the discussion session of the *eighth week*, special regulations in schools regarding freedom of and limitations on speech were argued. Some of the students advocated the extended speech limitation should be employed in the schools. They claimed that in addition to legal borders of free speech, politics related speech should also be banned. The other students supported the speech rights of both the students and the teachers. They concerned that any speech could be considered as politics and banned. The uncertainty on the borders of limitations on speech was also discussed.

At the discussion session of the *ninth week*, the students gave different examples of addicted behaviors, such as video addiction, programming addiction, or game addiction. They also talked about addictive games and shared their avoidance

strategies. One of the students highlighted that almost all educational resources exist on the Internet. The reason for excessive computer use was generally related to the studying process. Extended amount of time on computers might result in addiction.

From the *eleventh week* of the semester, cybersecurity-related topics were started. Before beginning the lecture, the researcher asked the students about some fundamental information security issues. How often they change their user code passwords, whether or not they use antivirus software were the two examples questioned in the session. Only one student in the classroom declared that he has regularly been changing his user password in every year. Majority of the students using antivirus software, and they complained about the infected computers in computer labs.

In the discussion session of the *twelfth* session; firstly, an online phishing activity in phishing.org was done. It was a 14-question test, which asks visitors whether the image on the screen was a phishing example or not. Most of the students were aware of phishing. However, some of them have mistaken to choose legitimate sites as phishing.

Then, several information security incidents the students observed or experienced were discussed in the classroom. The most frequent security incidents the students told about were related to financial issues, such as ATM or POS cracking events.

In the discussion part of the *thirteenth* session, the students' password management preferences were discussed. One of the most significant contributions was related to safe password requirements. The students had different strategies on memorizing passwords of different accounts. One of the students suggested that he set the same password for all of the accounts he signed in. Some of the students stated that, with the inclusion of two-level authentication, they were not trying to memorize the password and each time they log in a system, they generate a new password with the aid of authentication system. The risks and benefits of these strategies were also discussed in the class.

4.2.2.5. Students' Online Participation in Both Implementations

The major topics, controversial issues, and debates were discussed in the forum pages. The major objective of the forum discussions was to increase the students' attention on the topic and to develop skills on thinking, discussing and expressing themselves about that specific topic.

Table 4.30. *List of the Forum Topics of the Two Implementations*

Main Topic	Time of the forum	Title	Nb. of Posts*
Security vs Safety	The First Imp. (I1) 5th week	Think about the words security and safety? What is the difference?	16
Information Security	I1 – 8th week	Please share and discuss information security scenarios.	17
Copyright	I1 – 10th week	Please present the major legal issues about intellectual property rights, copyright, and trademark in Turkey?	8
Academic Integrity	I1 – 11th week	Similar Thesis example	10
Privacy Issues in SNS	I1 – 13th week	Sharenting – Oversharing	8
		Student-Teacher SNS Friendship	12
Cyberethics	The Second Imp. (I2) 2nd week	Compare Legal, Moral and Ethics concepts. Specify examples that supports or contradicts each other.	10
Academic Integrity	I2 – 3rd week	Write your own code of ethics statements	11
		Similar Thesis example	2
Privacy Issues in SNS	I2 – 6th week	Sharenting – Good or Evil?	12
	I2 – 7th week	Teachers' interactions issues on the Internet and Social Media	12
Free speech Discussion	I2 – 8th week	Limitations of Free Speech	9
Information Security	I2 – 11th week	Please share and discuss information security scenarios.	8
	I2 – 13th week	A Privacy Breach example	6

**: The instructor and the researchers' posts are not included.*
"I1" and "I2" stand for the First and the Second Implementations respectively

The students were not willing to participate in forum discussions. The primary reason according to their responses was their false belief that it does not affect grading. Although the effect of participation grade, and how it was calculated were explained in detail, the students' tendency to be informed that each "homework" caused online

participation to be lower than expected. The responses were posted at last few weeks of both semesters. Information security scenarios and protection measures were the most responded forum discussion for the first implementation. The sharenting related discussions and student-teacher interaction through SNSs were the most popular topics of the second implementation. The summary of the forum titles is presented in Table 4.30.

4.2.3. Instruction Related Design Issues

There were several issues the instructor took into consideration. The contents, selection of subtopics and examples, method of instruction, and moderation of the discussion session were the critical points.

4.2.3.1. Instructional Issues in Lectures

The differences between the two implementations were not limited to the change in the content sequence. Some topics that could not be explained sufficiently in the first implementation were lectured in more detail. They were free speech and addiction.

In the first implementation, the term freedom of speech was given in 3 brief sections; (i) the definition of freedom of speech, (ii) Article 26, the constitutional statement in Turkey, and (iii) hate speech. It was a part of the last session. Cyberbullying and addiction topics were also given in the same session.

In the second implementation, the lecture covering freedom of speech was given in a lecture session. The lecture included 5 main sections namely, (i) definition of freedom of speech, (ii) the constitutional statements, which were not limited to Turkey, the EU and US statutes and their overlaps and distinctions were also included, (iii) symbolic speech, (iv) limitations of freedom of speech, and (v) freedom of speech on the Internet and anonymous users were included in the lesson. Hate speech was included in the limitations of freedom of speech. The lecture concluded with the discussion of free speech issues in the educational setting. It was discussed in the discussion session that week.

In the first implementation, the term addiction was given in 3 brief sections (i) the definition and addiction types, (ii) signs of addiction, and (iii) avoidance strategies. It was a part of the last session. Free speech and cyberbullying topics were also given in the same session. In the second implementation, lecture covering addiction was given in a lecture session and included four main sections, (i) stages of addiction, (ii) computer addiction types, (iii) signs and effects of addiction, and (iv) strategies to avoid and cope with addiction.

The labels of the addiction stages are as follows; first use, continued use, tolerance, dependence and addiction. These stages explain alcohol, drug or any other addictive substance addiction. However, addictive behaviors through the use of computers, such as surfing the net or playing online games also follow these steps. Based on a paradigm that addiction is a physical change in the human body, the term "behavioristic addiction" is a controversial issue among psychologists. One idea claims that cyber addiction is explained as the individual's dependence on dopamine and can be explained as dopamine addiction. The opposing idea claims that insisting computer-related behaviors are behavioral disorders but not a physical addiction. The researcher explained about these controversial issues in the lecture briefly.

Being a digital citizen brings us the responsibility to know about the legal statutes. "The Law on Regulating Broadcasting on the Internet and Fighting against Crimes Committed through Internet Broadcasting," commonly known as the "Internet Law" or Law5651, was a rather complicated issue for an end user. In the course, two parts of the law, *Definitions* and *Content Provider* were explained in detail. The legal responsibilities of being a content provider were also explained.

Acceptable use policy, code of ethics and honor code were contextually dependent topics. Since the students were the pre-service teachers, after explaining the definition and general details about these terms, the researcher explained the University's "*Code of Ethics and Core Values*" statements and the directives of MoNE.

Similar to the case of freedom of speech, a lecture about cyberbullying required psychology and law knowledgebase. In a non-educational context, it would be sufficient to define and classify cyberbullying and explain what a victim can do in case

of a cyberbullying incidence. However, in an educational context, both the potential victims and bullies might be the students. In other words, a different approach is required. Education aims to win both individuals in such cases.

For this reason, in addition to informing the victim of cyberbullying, the course content should be arranged for the student who is in the "bully" position. Cyberbullying is a different situation from bullying in a way that, the school authorities can detect bullying behaviors that occur in the school environment. It may have disciplinary results. On the other hand, if the threat occurs through the internet, to take disciplinary action may not be easy unless the internet resources provided by the school are used for bullying. Preventing cyberbullying is an ethical concern. To inform the students about the effects of inappropriate online behavior and to provide peaceful honor code principles may prevent such cyberbullying behaviors. The counseling services of the school should examine the psychological effects of bullying. The researcher prepared the course in the way that she explained these in detail in the course.

The printed materials or e-books were explaining the addiction content in in-depth technical detail, and it was either not suitable for the prospective students or possible to explain in a one-hour lecture session. However, there were many online sources from Non-Governmental Organizations (NGO) and Non-Profit Organizations (NPOs).

Classifying the addiction types were another challenging issue since there was no consistent labeling to define the term computer related addiction. Cyber addiction, computer addiction, internet addiction, mobile addiction or game addiction were the most frequent labels which describe the types of the term, cyber-addiction. Game addiction was a part of a computer or mobile addiction. Mobile addiction was also a part of computer addiction. All these types have similar addiction indicators. There is an increased demand for the use of mobile devices. Since mobile devices have plenty of affordances in daily lives, one can easily become mobile addicted. The content-based differences between the two implementations are presented in Appendix 0.

4.2.3.2. The Variety and Daily Life Correspondence of Examples

Two most cited issues the learners pointed out were the variety of examples and daily life correspondence of the topics. The students were in favor of the various examples given during the course. The examples were about the daily lives of hot topics in the news. Most of the students emphasized that the examples were eased the topics to be understood.

> For example, you supported with various examples and gave concrete examples, so that I understood. I did not think it would be understood then; I thought I would have difficulty to understand; it was not as I have concerned (M102).

> *Derste mesela zaten, siz sürekli somut örneklerle desteklediğiniz için anladım. O zaman da düşünüyordum dersi alırken bu kadar oturacağını düşünmüyordum, çok daha zorlanacağımı düşünüyordum, beklediğim gibi olmadı (M102).*

> … I think in all subjects you think about the examples you give and the points you want the students to think about, for example, that you have a very good point to make a question mark for us (M207) ...

> *...tüm konularda da bence verdiğiniz örnekler ve öğrencilerin düşünmesini istediğiniz noktaları, mesela o konunun bizde de soru işareti oluşturması için çok doğru noktalara değindiğinizi düşünüyorum ben (M207)...*

> Real life examples. Examples were every day. It was a nice and pleasant experience for me to transform education into a visual, and to give examples of intangible concepts with real concrete examples (M105).

> *Gerçek yaşam örneklerinin olması. Örnekler günlük yaşamdandı. Eğitimin görsele dönüştürülmesi, somut olmayan*

kavramların görsele dönüştürülüp gerçek örneklerle anlatılması benim için güzel ve hoş bir deneyimdi (M105).

Examples of daily life were beneficial. It was useful because it was a matter of life, and every week we supported the topics covered in that session with such examples, it had consistency (M106).

Günlük hayattan örnekler verdiğiniz için yararlı oldu…Hayatla iç içe bir konu olduğu için ve her hafta konuları böyle örneklerle desteklediğimiz için yararlı oluyordu, tutarlılığı vardı (M106).

4.2.3.3. Instructional Issues in the Online Environment of the Course

The students were able to log in to the web site by using their user-codes and passwords defined for the university computing services. Since they did not expect to memorize another user account and password, this was a good point for logging in to the course web site. On the other hand, some of the students stated that they preferred to log in the campus-wide course management system and forgot following the original course web site which is located in the CEIT server.

Students are using ODTUClass. But they do not log into the course web site. They can forget. It is a bit disturbing being in another platform (M104)…

Öğrenciler ODTUClass kullanıyor, ama dersin sitesine çok sık girmiyor, unutulabiliyor… Farklı platformda olması biraz sıkıntı (M104)…

There was a problem in the notification settings of the web site. When a new forum post was added, or a new file was uploaded, an automatic notification was not always sent to the students. For this reason, for each post or uploaded file on the course web site, the students were notified manually through e-mail.

There were two projection screens in the classroom, which was beneficial for all the students to see the presentation. The researcher was expected to operate both

projectors for each lecturing session, adjusting the screens, and operating the projection devices. All these technical details sometimes confused the researcher. The board near the desk was a touch-sensitive smart board. It was affected by the researcher's accidental touch.

The computer in the lecture room was locking down when running a video in presentation software. As a result, the researcher had no chance to enrich lecturing materials with audiovisual tools. Audiovisual materials were presented separately. The students also noticed the deficiency of visual and animated details, and two of the participants who enrolled in the second implementation suggested the inclusion of visual and animated tools to enrich the course.

The researcher observed that the students were not keen on reading the materials. In some cases, some of the students explicitly stated that they did not prefer readings. It affected discussion sessions of each week negatively. The reading materials were found to be too long, and it was said that it would be better if they were shortened. The majority of the students stated they did not read. Only a few students who stated they read, all were FLE students, confirmed that they were long and could get students bored. In the second implementation, the researcher added extended lecture notes for the students; they were uploaded to the system after the lecture given. One of the students suggested that these lecture notes should be visible before the session, so that the students may prepare for the lecture. The feedback from the students obtained by observations also confirmed the need for the detailed but brief lecture notes. For this reason, the researcher prepared an extended summary of each week for the second implementation. One of the samples is presented in Appendix L.

4.2.3.4. Suggestions from the Students

The interview participants have a variety of suggestions to advance learning the contents. There was no homework in the grading policy for none of the implementations. Two participants claimed that homework could be included. Inclusion of group works (suggested by five students out of 23) and in-class interactive activities was also suggested.

In-class discussions had a positive effect on the participant's course related thoughts. However, the duration of the discussions might be controlled. In the second implementation, the enrolled students were from two departments, which were FLE and CEIT, and almost evenly divided. The students of both departments demonstrated high-quality participation in both lectures and discussion sessions. Especially, in the subject of cyberethics, their approaches to the cases which could be evaluated from different perspectives were at a level which could improve the quality of the course. Interviewees said that they were also satisfied with these in-class debates. They also added that they had a chance to be exposed to different perspectives.

> There were FLE and CEIT students in the classroom. Sometimes we learned from them; sometimes we contributed, it was nice (M202).

> *Sınıf içinde fle ve ceit vardı. Biz onlardan yeri geldi bir şey öğrendik, yer geldi bir şekilde katkıda bulunduk Bu güzeldi (M202).*

> Discussion sessions were valuable, so that we could learn. One can forget if teacher only explains. Even I do not speak, when my friends talk, I can observe they think different, and a can better memorize. I think they (discussions) were good. But it was sometimes long, sometimes short, it would be better is the duration were specified (M204).

> *... Discussionlar (Tartışma seansları) değerli, hem daha kalıcı oluyor. Sadece anlatıp geçince unutulabiliyor. Ben konuşmasam da başkaları konuştuğunda da aa daha farklı düşünüyormuş benden diye gözleyince daha akılda kalıyor. Bence gayet iyiydi. Ama bazen çok uzun bazen kısa oluyordu. Onun süresini belirlemek gerekir. (M204).*

Participating either in-class activities or online activities was not compulsory. It was included in the grading policies of both implementations. Some interviewees stated that the effect of participating in online activities, and in-class discussion on

grading was not understood. It was considered as same as attendance. However, grading of participation, the effect of which was 10%, was the combination of in-class participation and online participation. Although the researcher often reminded the importance of in-class discussion on understanding the topics clearly, those who did not prefer to participate in the in-class discussion or online forums complained about their grades, saying they were lower than they expected. In the second implementation, this was explained to students more clearly.

The classroom was one of the largest rooms in the building, and the researcher adopted "the first three rows" rule in the second implementation. Although the purpose of the study does not aim at classroom management related issues, it was observed that the sparse sitting of the students negatively affected in-class participation and following the lectures in the first implementation. For this reason, the 20 students in the class are made to sit in the first three rows. One of the interviewees pointed out that he did not like the rule at the beginning, but he also added as he participated in the in-class discussions, he realized how effective and beneficial this rule was.

The interviewees have critical suggestions for effective use of discussion forums. Forum participation was lower than the researcher's expectations. Three students recommended to include controversial issues as forum discussion topics and all forum topics might be in only one head topic, so that it would be easier to follow the forums for the students.

> The students are not used to participate in forums. If there were a few controversial topics, more students would participate in forum discussions. However, the students tend to approve whatever you say (M203).

> *İnsanlar foruma alışık değil hocam. Birkaç tane controversial issue olursa daha iyi katılım olabilir. Bir de insanlar siz ne derseniz kabul eden bir şey yazıyorlar(M203).*

> Participation in forum discussions was very insufficient. Instead of defining different forum discussions for each week, it would be better if you have defied a major topic and include each discussion

under that topic. The students confused in choosing which forum discussion to write in. Forum posts were not like a debate. Everyone wrote his/her post but did not respond to other's posts. (M206).

Forum çok yetersizdi, belki çeşit çeşit forum olacağına tek bir forum altından gitse daha iyi olabilirdi. İlk başta nereye yazacağımı bilemedim, forumu kaçırıyorduk. Forum katılımı düşüktü. Tartışma gibi olmadı, herkes bir şey yazdı ama kimsenin altına ben öyle düşünmüyorum gibi bir şey olmadı… birbirine cevap yazmadı (M206).

I do not think forum discussions were used beneficially. Every student wrote his or her idea but did not discuss other students' ideas. Each student presented his/her point of view. I think the forum would be more useful if it would be used effectively (M208).

Forumlar yapmıştık, ben onların çok faydalı olduğunu düşünmüyorum. Çünkü herkes kendi fikrini yazdı orda ama bir tartışma ortamı yaratılamadı orda, herkes konuyla alakalı ama farklı yerden vurguladılar konuyu. Forum anlamsız değil de biz onu etkili kullanamadık diye düşünüyorum (M208).

The online environment of the course was located in a local learning management system (LMS), rather than campus-wide LMS, which the students were more familiar with. It was one of the reasons for the students not contributing to the course's online activities. Furthermore, despite in-class and forum discussions, the students perceive this course as an instructor oriented course and expect to be more involved in course-related activities.

4.2.4. Summary of the Theme

"*Design issues*" theme mainly answered the first research question;

"What are the key factors encountered during the design and development of a course in an attempt to raise the pre-service

teachers' information security awareness and cyberethics sensitivity?"

The major issues emerged in the scope of design issues were the multidisciplinary nature of the course, and the how critical issue was the content sequence. In the second implementation C3 framework (Pruitt-Mentle, 2010) is employed. Each subtopic of C3 has a multidisciplinary nature. The lecturer of such a course is supposed to have sufficient knowledge in these areas such as cyber addiction, cyberbullying, and freedom of speech, copyright. The printed sources in information security are mostly addressing IS professionals or managers. Addiction and copyright-related instructional materials also address psychology or legal experts respectively. An introductory level textbook is also necessary.

The prior knowledge of the students was not homogeneous. However, since they were digital natives, they have a familiarity about security issues of SNSs. The course was designed without any assumption of prior knowledge. However, the students who were more familiar with the topics felt more confident in the lecture. The students of CEIT department were familiar with the topics, whereas the students of other departments were not. Another critical issue about the learners was that they were unwilling to reading.

The course included a 1-hour lecture, 1-hour discussion session each week. Besides, the students supposed to participate in weekly forum discussions. The lecture notes included a general definition and descriptions of the examples of the terms about the issues of the corresponding week's main topic. The students were able to participate in the lecture session. They were able to ask questions or provide examples to advance the lecturing sessions. The discussion sessions included a highlighted theme about current week lecture. The students were able to contribute to these in-class activities. The forum discussions included one or two controversial issues. The students were expected to develop their ideas and express them in writing. A summary of the findings of this theme is presented in Table 4.31.

Table 4.31. *Summary of Findings for Research Question 1*

The key factors encountered during the design and development of a course in an attempt to raise the pre-service teachers' information security awareness and cyberethics sensitivity	
Content related Issues	• Content Sequence: Briefly Cyberethics, Cybersafety, Cybersecurity. • Multidisciplinary Course. • Deficiency of instructional materials for pre-service teachers
Learner related issues	• The students' prior knowledge. o The majority were familiar with SNSs related privacy issues. o CEIT – Non-CEIT difference. o The most participated lecture session was about mobile security • The students' unwillingness to read.
Instruction related issues	• The lecturer of such a course is supposed to have sufficient knowledge of C3 topics. • Variety of examples and daily life correspondence in lecture contents is essential. • The lecture should address different areas of interest. • The forum page allows students to develop an idea about the subject and to express it in writing.

4.3. Facilitators and Challenges

The theme "*facilitators and challenges"* was another theme that emerged from the qualitative study. Different factors affected the implementation process. The facilitating and challenging factors which the researcher encountered were presented in the following sections. First, the facilitating and challenging factors from the instructor's perspective were presented. Later, how the challenges are handled were explained. The facilitating and challenging factors from the students' perspective are presented at the end of the section. The findings gathered from designer reflections, field notes, and the interviews are presented in each section.

4.3.1. Facilitators from the Instructor's Perspective

The topics taught in the course, and the examples given in the lectures were part of the current news and events. The students' participation, questions and contribution the course was influenced by this correspondence.

4.3.1.1. Daily Life Correspondence

The topics of the course have a direct relationship with the students' daily lives. Besides, the current events had important contributions to the course. For instance, privacy issues in social media were explained at the same time with the "Mark Zuckerberg's Facebook Privacy Breach." In the meantime, some students think that they keep their information in private by turning off the display settings in social media accounts.

Internet-based applications are in our lives. The students have the opportunity to apply some of the subjects that they have learned in the course. They stated that having the opportunity to immediately apply what they learned was a facilitating aspect of the course.

The pros-cons discussions occurred in the lectures were liked by the students. Through these discussions, students had a chance to think about the issues which they had not thought about before.

4.3.1.2. Learners' Being Digital Natives

Since they were digital natives, the students were familiar with most of the topics covered in the course. It was also approved in their responses to newly learned topics which were explained in Section 4.4.1 in detail. The students were eager to learn C3 subjects. Being digital natives, they always had a lived or observed experience about the topics covered in the course.

Cybersecurity, with which the students stated as they were least familiar, they could immediately contribute what they learn into their lives. The most remarkable example was the explanation of mobile security and permission issues of mobile applications. In both implementations, soon after the permission issues were explained, most of the students in the classroom were started to check their permissions and question whether those permissions were necessary or not. The topics covered in the course has a contribution to the students' lives.

4.3.2. Challenging Factors and How They are Handled

Throughout the design, development, and the implementation of this course in both implementations, the researcher encountered several problems. The challenging issues and remedies were explained in related sections. In this section, a summary is presented.

In the first implementation, the students were unwilling to read. During the first implementation, in the second half of the semester, the presentations included detailed explanations, while at the beginning of the semester short phrases were included. Besides, the researcher provided extended lecture notes for the second implementation.

Extended lecture notes did not solve the weak reading habit problem. The researcher ensured that the details about the topics which were not covered enough in the presentations were given to students in more detail.

The interviewees complained about their English speaking level and felt inadequate to participate in an English-medium course. The perception of deficiency in English prevented them from participating in in-class discussions and lectures. In the second implementation, the researcher gave brief information in Turkish, and this raised the in-class discussions and lecture participation.

The low participation in the forum was another challenge. It was solved by giving more detailed information about the participation grading policy and informing the students that both in-class and forum participations have a direct effect on their participation grades. Grading was not the only motivation for the students to participate in forum discussions. In some lecture sessions, the researcher talked about a discussion post and raised attention on forum discussions.

There was a problem in the configuration of the computer in the classroom, where the lecture was given. The researcher was unable to run a video during the presentation because the computer crashes. It could not be solved during the semester. For this reason, the researcher presented the audio-visual materials at the end of the lecture sessions.

During the implementations, deciding to what extent the contents would be explained was another challenge. The multidisciplinary nature of the course was described in the previous section. However, the existing instructional materials were addressing IT professionals, information system managers rather than end users. The copyright-related course materials, likewise, addressing the legal professionals or copyright holders. For each topic, the sources were reviewed, simplified and course contents were prepared.

4.3.3. Facilitators and Challenges from Learners' Perspective

The students were asked their liked and disliked aspects of the course. The language was one of the significant predictors of the two implementations. In both implementations, the course was given in English whereas the discussion part was run in Turkish. The instructional materials, such as lecture notes and recommended readings were English. Besides, the language of the forum discussions was also English. In the second implementation, the researcher gave an extended explanation of the topics in Turkish. The increased native language support has influenced the students.

For this reason, the language of instruction was stated to be a challenging factor, particularly by the first implementation interviewees. Overall, eight students, of the first implementation, stated that they had difficulties in understanding the terms, but the researcher's explanations in Turkish cleared the confusing topics. They also added that they could feel more comfortable while participating in the class discussions. Some relevant responses are given below as an example.

> I think English was a challenge. Maybe it was about me. When it (the course) was in English, and also verbally, it seems like the contents are disintegrating during the lecture conversation (M112).

> *Hocam, bence İngilizce konusu zorlayıcıydı. Belki benden de kaynaklı olabilir, Ingilizce oldugu zaman ve bir de sözel olunca, sürekli konuşunca bir yerden sonra konu dağılıyor gibi oluyor (M112).*

> For example, CEIT students have become accustomed to those (*cybersecurity-related, or technical*) words, they probably can understand. I am familiar with the mathematics terms in English as a mathematics student, for example. However, I could not understand the terms of this course. When we did not understand, we were passing Turkish or something; I think it was good, I could understand then (M113).

> *Mesela terim olarak BÖTEciler alışmıştır o kelimeleri, anlıyor, mesela ben matematikçi olarak matematik terimlerinin ingilizcesine alışkınım. Ama bu dersin terimlerini ama ben anlayamıyordum. Anlamadığımız zaman türkçe falan geçiyorduk ya, bence gayet iyiydi, o zaman anlayabiliyordum (M113).*

> I like the fact that the explanations of the course were in Turkish. I felt very comfortable in our native language, while both are attending the class and participating in the lectures. We used a language as a combination of English and Turkish in the discussions; it was beautiful. We did not have any problems with the exam because other sources such as the lecture notes, reading materials, etc. were also in English (M202).

> *Dersteki açıklamaların Türkçe olmasını çok beğendim. Anadilimizde çok rahat hissettim, derse gelirken de, katılırken de… Tartışmalarda Türkilizce bir dil kullandık, bu güzeldi, ders notları, okumalar falan, diğer kaynaklar da ingilizce oldugu için sınav konusunda da sıkıntı çekmedik (M202).*

The major characteristics of the course which the participants commonly highlighted as the most favorite aspect was the *real-life correspondence of the course*. The participants also mentioned that the course addressed all subject teachers and not limited to CEIT. Relating information security and cyberethics related topics to daily life experiences was also one of the objectives of the course.

Addressing the different examples including daily life correspondence was another good feature of the course which increased the students' interest. The researcher provided different materials from different sources such as video links, newspapers, and articles. Two students also highlighted this detail.

> We have chatted about daily lives. At the end of the lecture, those were more memorable. You showed pictures of daily lives at the end of each lecture. They were my favorite things. It was a social course. I feel relaxed among all the loads of other courses. It both taught (*the course topics*) and relaxed (M206).

> *Günlük hayattan sohbet etmemiz hocam. Ders sonunda, Bence onlar daha akılda kalıcı, Hatırlamaya yönelik, her dersin sonunda günlük hayattan fotolar gösteriyordunuz. onlar benim en beğendiğim şey oldu derste. Sosyal bir ders oldu. O kadar dersin ağırlığının içinde rahatlatan, hafif geçen güzel bir ders oldu. Hem öğretti hem rahatlattı da (M206)...*

> It was in a chatting mood. Everyone could express his or her idea. The examples you give from daily lives. These were the points about the course I liked the most (M208).

> *Sohbet havasında olmasıydı, herkesin fikrini söyleyebilmesiydi. Günlük hayattan da örnekler verebilmemiz birbirimize konuyla alakalı, bu yönden güzeldi (M208).*

The researcher provided different definitions from different sources of information. Particularly, for the information security topics, the terms were presented both in non-computer related meanings and definitions and technical definitions. Three students (out of 23 students) highlighted that they could easily understand when they were able to read the definitions from different sources.

Lecture presentations were found to be clear and complete by some students, whereas some other students complained that they were insufficient to understand. In the first implementation, the researcher assumed that the students would follow the

reading assignments and brief summaries as the lecture presentations would be sufficient for the students. Lecture presentations would provide a limited summary of the topics. The researcher included only the titles of the subtopics, included some generic definitions. Then, she explained the topics in the lecture session in detail. She provided recommended readings for all topics. At this stage, it is remarkable that the students who complained about the insufficiency of the lecture presentations enrolled in the first implementation stated that they did not read the recommended readings.

The extended lecture notes were prepared for the second implementation. Furthermore, additional reference materials have been proposed in the recommended links section of the course website each week, as in the first implementation, to provide a more detailed understanding of the topic. At the end of each lesson, the researcher reminded the students of these reading materials.

The reading materials generally had 8-10 pages. However, in some cases, a book chapter or a report might be recommended. In that case, the researcher highlights the most critical part of that source. For example, a 200-page report was presented to the students when Freedom of Speech topic was taught. The researcher focused on the last section, the freedom of speech issues through the internet. It is clear that the students do not wish to be responsible for substantial amount of reading materials in an elective course, in addition to their natural course load.

In the first implementation, the researcher presented the topics about information security in detail. For this reason, some of the cybersecurity-related topics were repeated in each week. For example, password security was given in the protection of digital identity, information asset, and mobile security. Some of the students complained about these repetitions. It was a side effect of an effort to explain the information security concept to the students in more detail. The content sequence related to information security was transferred to a second period with a smoother subject flow that prevented repetitions.

The interviewees generally complained about the difficulty of *memorizing the terms*. The course was not based on memorization. It was a matter that the researcher cared about. On the other hand, it was revealed that subjects should be better explained

so that the students can understand the topics. Three of the students stated that they had difficulty in memorizing creative commons abbreviations.

4.3.4. Summary of the Theme

"*Facilitators and challenges*" theme mainly answered the second research question;

> *"What are the possible facilitating and challenging factors for the design, development, and implementation process of the course?"*

This course had a critical role in raising pre-service teacher's information security awareness and cyberethics sensitivity. The importance of information security affected the interest of the students. Daily life correspondence was one of the most critical facilitators both for the students and the instructor. For each topic, the instructor was able to provide an example citing recent news or current event. The students were familiar with the given examples, and they could contribute to their lived experiences or observations. The learners were digital natives. Although the non-CEIT students have concerned about a computer-related course at the beginning of the semester, they could apply what they learned in the course easily in their daily lives.

On the other hand, the students' unwillingness to read and to participate both in class activities and forum discussions was a challenge for the instructor. Extended lecture notes were prepared for the second implementation. The forum participation was encouraged by an explanation of the effect of participation on grading policy. The lack of instructional material covering C3 topics was one of the reasons for this study. On the other hand, reviewing different sources to develop weekly lecture notes and deciding to what extent each topic would be explained were the challenging issues for the instructor.

The learners highlight the friendly environment of the lectures increased their interest in and participation in the lectures. The variety of examples and different source of definitions were the other factors the students mentioned they were in favor of. However, English-medium course was a challenge for them. Being unfamiliar with the terminology and trying to memorize the terms were the other challenging issues.

The instructor explained some of the topics in the native language and the students acknowledge this as a facilitating issue. A summary of the findings of this theme is presented in Table 4.32.

Table 4.32. *Summary of Findings for Research Question 2*

The possible facilitating and challenging factors for the design, development, and implementation process of the course.		
Facilitating Factors for the Learners	• Daily life correspondence • Learners were digital natives • Native language support • The friendly environment of the lectures • Variety of examples and different sources provided to the students	
Facilitating Factors for the Instructor	• Daily life correspondence • Learners were digital natives	
Challenging Factors for the Learners	• Students' English Profession Level	• Extended native language support
	• Inadequacy of computer literacy	• A glossary of the terminology would be provided
	• Memorizing the terms	• Hands-On activities would be included in instruction so that the students were able to meet practical correspondence of some of the terms.
Challenging Factors for the Instructor	• Students' weak reading habit	• Extended lecture notes were prepared.
	• Students were unwilling to participate in class activities and discussion forums	• The effect of participation is explicitly explained. • The forum discussion responses were acknowledged in the following weeks.

4.4. Potential Contributions of the Course

The major theme that emerged from the qualitative analysis of the study was the "potential contributions of the course." The data sources of this theme include the researcher's field notes and interviews.

Five sub-themes, appeared from the *potential contributions* are; (i) via the course, the students' newly learned topics, (ii) corrected misconception they had, (iii) raised awareness on cyberethics, cybersafety and cybersecurity, (iv) perceived

contribution of the course to the prospective teachers' teaching profession, and (v) effect on the students' daily lives such as password management strategies, or mobile device usage.

4.4.1. Newly Learned Topics

At the beginning of the interview; the students were asked whether there were any topics they have learned for the first time in this course and if so which topics they were. Eight of the 23 students stated that they had seen all of the topics for the first time in this course. For example, the interviewee M108 stated that almost all topics were new and highlighted that it was necessary to learn these topics for every individual.

> There is none (*of the topics I have seen before*) indeed. Cyberethics, computer related issues, these all are new areas for me. We are living in the 21st century, a technology era, every individual has to know the contents of this course. 90% of the contents of this course were new for me (M108).

> *Aslında yok. Cyberethichs bilgisayar… hani bunlar bana çok yeni alanlardı. 21.yyda yaşıyoruz, teknoloji çağında yaşıyoruz. Her bireyin bu dersin içeriğindeki bilgileri bilmesi gerekiyor. Öğrendiğim %90'ı benim için yeni bilgiydi (M108).*

Almost all students stated that they had learned most of the topics for the first time. For example, the interviewee M110 said he had heard about some of the topics in cyberethics area; he has seen nearly all topics covered in this course, even in the cyberethics area, for the first time.

> In general, nearly the all topics were new to me. We knew that passwords have to be changed in a proper frequency. Some of the main topics in cyberethics… We probably have heard about cybersafety issues. Everyone has known they were required to be careful about (*cybersecurity*) related issues. But it was the first time I have seen these topics in detail. I have seen all topics for the first

time, such as (*ISO*)27000, (*The Internet Law*) 5651, and the hacker types. I have seen for the first time most of the things (M110).

Genel olarak hemen hemen hepsi yeniydi.Passwordun sık değiştirilmesi gerektiğini biliyorduk. Belli başlı bazı şeyleri biliyorduk siber etik anlamında…Belki genel anlamda güvenliğimiz konusunda bazı kavramları duymuştuk ama terimsel olarak adlarını yeni öğrendik. Genel olarak dikkat etmemiz gerektiğini herkes biliyordu, ama daha detaylı ilk kez gördüm. Hepsini ilk kez gördüm… 27000i ilk kez gördüm. 5651 i ilk kez gördüm. Hacker typelarını ilk kez gördüm.Çoğu şeyi ilk kez görmüşüm (M110).

Twelve of the 23 interviewees highlighted that they were familiar with some of the concepts covered in the course, but they have a chance to learn the *names of those topics*. For example, the interviewee M207 mentioned that hoax and clickbait were the most familiar incidents he faced with, but he did not know their names. As other examples, the interviewee M101 and M112 highlighted that they were familiar with some of the topics, such as phishing but had no idea of potential risks of it.

I was familiar with the topics, but I have not learned in this detail, or I did not know their names. Clickbait or spam e-mail, we can see every day on the internet, but I did not know how dangerous it could be or what it's name. I have learned. It was nice for me. I thought I knew copyright (M101).

Aşina olduğum konulardı ama bu kadar derinine inmemiştik, ya da adını bilmiyordum. clickbait, ya da mesela gelen spam mesajlar hergün nette karşılaşıyordum ama boyutu ne derece tehlikeli olabildiğini ya da adı ne bilmiyordum. Öğrenmiş oldum. Güzel oldu benim için. ... Copyright bildiğimi düşünüyordum (M101).

I could not know the names of the topics, technical labels, specifically. We, certainly, know how security measures are taken, how to choose a strong (*hard-to-crack*) password, how to identify

> fraudulent content. These were confirmed with the course. The name phishing is not important; I learned not to click each mail (M112).
>
> *Spesifik olarak bir şeyleri isim olarak bilemezdim, teknik isimlerini bilemezdim. Tabii ki bilgisayarla ilgili güvenliğin olması gerektiği, şifrelerimiz kaliteli olması gerektiği, internette bazı dolandırıcılık, sahte mailler gibi tahminini yapıyorduk. Biliyordum yani sağdan soldan Derslerle de tasdik oldu, teknik ayrıntılarını gördüm. Adının phishing olması önemli değili ama her maile atlamamak gerektiğini öğrendim (M112).*

The students highlighted that having an idea about what a term means was not enough to declare that they knew the topic. Thirteen of the 23 students stated that they thought they knew most of the topics but had a chance to learn in detail. They also emphasize that they had a chance to learn some of the topics in detail which they have heard about. For example, the interviewee M205 addressed the value of learning the terminology:

> There were (*some topics I have heard before*). I knew as "made-up news" and have learned that its name was Hoax on the internet. I have heard about most of the content. However, I have learned the terminology in this course. We knew the concepts, but have difficulty in explaining them. Now we have learned so that we could explain (M205).
>
> *Vardı, ben asparagas haber olarak biliyordum, ama internet ortamında hoax dediğimizi burda öğrendim. Bu içerikleri biliyordum, içeriklere aşinaydım, ama terminolojiyi burda öğrendim. Kavramları biliyorduk, açıklamakta güçlük çekiyorduk artık açıklayabilecek kadar öğrendik diyebiliriz (M205)…*

The classifications of the concepts were also essential learning outcomes of the course according to the interviewees. For example, five of the 12 CEIT students stated they knew hackers but did not have any idea of their types. In particular, the term *ethical hacker* (commonly known as *white hat hacker*) was new to them.

Similarly, *Malware types* or *attack types* were also the subtopics that the students learned in detail in CEIT 215. Most of the students stated that they had heard about addiction. However, they stated that they learned the addiction stages and the physical and psychological effects of addiction in this course.

Table 4.33. *The list of topics in the sub-theme of newly learned topics (Some of the most cited responses)*

Phrase	Frequency
The names of the terms covered in the course [a]	12
Concepts in detail	11
All of the topics	2
Copyright related details [b]	21
The Law 5651	5
Controversial Issues of Ten Commandments	3
Freedom of Speech (*speech types and limitations*)	3
Citation issues and Plagiarism Types	2
Code of Ethics and Honor Code	2
Hacker and attack types [c]	7
Phishing and Password Protection strategies	5
ISO 27000	3
Hardware Security	2
Mobile Security	2
Virus	2
Fraudulent Content [d]	11
Social Media Privacy [e]	9
(*The Stages of*) Addiction	3

a: These students said that they were familiar with the concepts in general, but did not know the terminology.
b: Fair use (12) Copyright duration (5), Copyleft (2), DMCA (2), Creative Commons (3)
c: White Hat Hacker (3), Hacktivists (1), Script kiddies (1)
d: Hoax (6) Clickbait (5) Fake profile (4)
e: Sharenting (4), Permanence and Effects of Digital Identity (2)

Briefly, the cyberethics topics, especially *freedom of speech* was a known topic. However, the *limitations of freedom of speech*, *symbolic speech* and particularly *hate speech* were mentioned to be the newly learned terms. Similarly, cyberethics and Ten Commandments of Cyberethics were also stated to be known by some of the

interviewees. On the other hand, they added that they have not heard about the controversial issues of Ten Commandments before.

Copyright is a popular topic. The responses of the interviewees also confirm this. However, fair use policy was a topic that most of the interviewees (12 students) stated that they have heard for the first time. The Copyleft movement, including free software foundation, open source community and creative commons licenses were also newly learned concepts in the topic of copyright.

To summarize, privacy and safety issues of SNSs and intellectual property related topics were the topics which the students highlighted that they had learned in this course. The list of the topics which the interviewees stated they have seen for the first time is presented in Table 4.33.

4.4.2. Corrected Misconception

The students were asked whether there was any topic they have used to know erroneously. In the interviews, the students responded to different answers. Among the responses, white hat hackers, self-plagiarism, and privacy issues of SNSs were the most frequent answers.

For example, five students stated that they had an idea about what plagiarism is; however, self-plagiarism was a surprising topic for them. The field notes also support this issue. Both in the first and the second implementations, on the week which *academic integrity* related topics were covered, when the researcher talked about plagiarism types and self-plagiarism, some of the students reacted and asked why it violates academic integrity and why their grades were decreased.

> Plagiarism types (*which I used to know differently*). For example, I did not know such a thing, that using our homework in another course (*homework*). My grades deducted. I did not know the self-plagiarism issue (M206).

> *Plagiarism type olabilir hocam. Mesela kendi ödevimize bilmiyordum böyle bir şey olduğunu, bir başka derste kullanmıştım, puanım gitti. Self plagiarism olayını bilmiyordum (M206).*

The students added that their attention to protecting their digital reputation has increased. One of the students highlighted that she had no idea about the effect on SNS posts through their future life.

> … I was not aware of how sensitive this issue (*social media posts*) was. It was a good point for me and my in-future professional life (M102)…

> *… social medyadaki paylaşımlarının onun da mesela profesyonel yaşamdaki kimliğini etkileyeceği konusunun farkında değildim mesela (M102)…*

The students were familiar with privacy threats in social media. However, learning the permanence of digital footprint and threats of oversharing on their digital reputation caused them to control their SNS use behaviors. Five of the participants said that they did not know the permanence and risks of digital footprint.

> Digital footprint, I thought it could be deleted. It was impressed me indeed. It is never deleted (M208).

> *Digital ayak izi, silinebildiğini düşünüyordum, O beni çok etkiledi ayrıca. Asla silinmiyor (M208).*

The list of the topics which the interviewees stated they have known in the wrong way was presented in Table 4.34. The listed topics in the table are not separated from each other. For example, the security issues about the mobile application may cause a critical effect on digital reputation. Privacy settings of SNS accounts and oversharing issues create a permanent digital footprint for the individual and affect his or her digital reputation.

Table 4.34. *The list of topics in the sub-theme of Corrected Misconception*

Phrase	Frequency
Thought that self-plagiarism did not violate academic integrity.	6
Thought that Privacy settings provide sufficient security	6
Thought that white hat hackers are malevolent hackers	5
Did not care about oversharing and sharenting issues	4
Did not know about the permanence of digital footprint and its and effects on reputation	3
Used to know hoax and clickbait were the same	3
Did not care about https[a]	3
Did not care about the permissions of mobile applications	3

a: *security protocol for web sites*

4.4.3. Raised Awareness on Cyberethics, Cybersafety, and Cybersecurity

The students were asked whether the contents they have learned in this course affected their daily lives. Besides, they were asked about those perceived effects. Briefly, the responses to this question demonstrate that they felt more literate about cybersecurity and cybersafety issues. Almost all students stated that the course changed their computer use and internet habits. They became more concerned when sharing information through social media, started to select hard to guess passwords, and increased their social media security settings.

> The posts (*to Social Networking Sites*) with a teacher title, for example. You uploaded a document as recommended reading, about the effect of a teacher's SNS posts on his professional life. I was not aware of how sensitive this issue was. It was a good point for me and my future professional life (M102).

> *Öğretmen kimliğiyle yapılan paylasımlar mesela, bazı şeyler yüklemiştiniz ek okuma olarak, bir öğretmenin de sosyal medya*

hesabı ve sosyal medyadaki paylaşımlarının onun da mesela profesyonel yaşamdaki kimliğini etkileyeceği konusunun farkında değildim mesela… Bu kadar hassas bir nokta olduğunu bilmiyordum, iyi oldu benim için alanım için de iyi oldu (M102).

I knew that we have to select a strong password but did not know we should change in certain frequencies. I have learned in this course that we should use special characters for the passwords (M115).

Bir de şey, password kolay kırılamayacak password oluşturmamız gerektiğini biliyordum,ama belli aralıklarda değiştirmek gerektiğini ve kesinlikle özel karakterler kullanmak gerektiğine çok dikkat etmiyordum, bu dersle öğrendim (M115).

In particular, they declared that they could easily recognize a phishing site or e-mail, or able to identify a secure web site. Two participants, who were the students of the first implementation, highlighted that the web site of the course was not secure. The course web site was secured in the second implementation. In the interviews, they mentioned secure sites as "https" site, which refers to a secure hypertext transfer protocol.

I am, particularly, more careful about spam e-mails. I am not clicking everything anymore (M104).

Özellikle spam maillere karşı daha dikkatli olmaya başladım. Her şeye tıklamamaya çalıştım (M104).

I increased the security levels of my SNS accounts. The sharing settings are limited to "Only Me." I once looking at the watches on the Internet. Then watch related ads started to appear. I noticed this after this course. I was not aware of this before (M113).

Sosyal medya uygulamalarımı "güvenli"ye aldım. Sadece ben olarak ayarlıyorum. Mesela internette saatleri inceliyordum, FB'da

saat reklamları çıkmaya başladı. Bunu dersten sonra farkettim, daha evvel farketmemiştim (M113).

I did not pay attention to "https" details (*a security protocol for web sites*) of the web sites I visited. I did not mind whether it was a secure connection or not. After the course, It is the first thing I notice. By the way, the web site of our course was not secure either (M101).

Güvenli olmayan sitelerdeki "https" lere dikkat etmiyordum, artık ediyorum. Bu arada bizim web sitesinin de https olmadığını farkettim. Ona da aşina oldum, eskiden dikkat etmiyordum. Artık güvenli olmayan sitelere bakmıyorum (M101).

Cybersecurity issues were the part where the students paid the most attention and increased their knowledge. They highlight that they take into account the permissions which mobile applications mandate to give.

While downloading the applications, I take a look at the permissions of that application, and if I feel unnecessary permissions, I do not download that application. I used to accept the permissions before, but I do not anymore (M108).

Uygulamaları falan indirirken bakıyorum, nelere izin veriyor falan. Ya da uygulamayı indiriyorum, kameranıza izin versin mi şuna izin versin mi falan… Onları hep bu dersten önce evet evet diyip geçiyordum, ama şimdi kabul etmiyorum (M108).

Having learned cyberethics concepts, they stated that they have been more sensitive to copyright issues, hate speech, and censorship in social media. Four students recalled the DMCA related information on removed video links in YouTube and reported that they knew the reason about this information after learning it in the course. Three students underlined the creative common license types and expressed they recognize those symbols while surfing on the internet.

> When I see the safe harbor and copyright infringement notices on youtube, I could not understand why video has been removed, but now I know it was a legal result of DMCA (M112).
>
> *Youtubedaki safe harbour, copyright infringement uyarılarını gördüğümde ilk zamanlar videonun kaldırılmasının sebebini anlamamıyordum, şimdi DMCA ile ilgili olduğunu biliyorum (M112).*
>
> I started to notice the license types and CC (*Creative Commons*) licenses. While surfing on the Internet, I can see CC-BY or CC-ND type signs and understand what they mean (M110).
>
> *Paylaşım lisansları ve CC sembollerini farketmeye başladım. Internette gezinirken CC-BY ya da CC-ND gibi semboller görünce artık ne anlama geldiğini biliyorum (M110).*

Cybersafety related topics were generally known by the students. However, the legal issues, such as "Don't Track Act" and MoNE directives were not familiar to them.

Majority of the participants stated that they had increased the security level of their social media accounts after the lecture which social media privacy issues covered. Cyberbullying and addiction are also other thought to be known topic. However, two of the students highlighted that how to take action in case of cyberbullying incidence was very important and critical information. One of them and his friend have been a victim of e-mail harassment, and with the information they learned in this course, they could take action and got the cyberbully punished.

To summarize, the students stated they were more literate. They reported that they had grown sense on security settings of web sites and phishing details in an e-mail or a web site. Not only secure web site or phishing issues but raising the security levels of their SNS accounts and preferences about mobile applications is an indication of their raised information security awareness. Furthermore, they highlight the fraudulent contents such as hoax and clickbait on the internet which, they have used

to see before, but now they know in detail. A summary of the responses is presented in Table 4.35.

Table 4.35. *The list of topics in the sub-theme of Raised Awareness on C3*

	Phrase	Frequency
Cybersecurity	Feel more literate about computer related issues	14
	Password frequency and selection	6
	Leaving a hardware	3
	Phishing	3
	Secure surfing in the Net	3
Cybersafety	Changed SNS habits	9
	Cyberbullying	4
	Fraudulent Contents	3
Cyberethics	Hate Speech	4
	Copyright and DMCA issues	3
	AUP and ToS Awareness	3

4.4.4. Perceived Contribution to the Teaching Profession

In the interview, the participants were asked the following questions about the in-future teaching profession: (i) “How would you use the information you learned in this course in your teaching profession?” (ii) “Do you intend to use social media in your teaching process?

Majority of the interviewees (15 of 18) stated that they would use what they learned in this course when they become teachers. Two prospective English language teachers said that including information security related contents into their instructional materials is an ideal method for knowledge transfer. The interviewees from different departments mentioned similar plans for informing their prospective students. These responses indicate their high-level professional ethics sensitivity indeed.

I can lecture “information security” as a subject in the course (M108).

Bilişim güvenliğini derste konu olarak alıp sunabilirim (M108).

Even if I'm a math teacher, I can make students aware of them (C3 topics). I'm going to be a secondary school teacher. Students think they have the right to do anything on the Internet. I can guide them about C3 related issues (M109).

Öğrencilere matematik öğretmeni olsam bile bunların farkındalığını kazandırabilirim. Ben ortaokul öğretmeni olacağım, Öğrenciler internet ortamında her şeyi yaparım sanıyor, o konuda yönlendirebilirim (M109).

I would give examples to children, especially those related to citations, and show the types of plagiarism. But more importantly, I teach the issue of cyber bullying. Or how to protect them when a message arrives, for example, if I work with young children, I teach them at primary level (M206).

.. bilhassa atıflarla ilgili çocuklara örnek veririm ve intihal çeşitlerini gösteririm. Ama daha önemlisi siberzorbalık konusunu öğretirim. Ya da kendilerine mesela bir mesaj geldiğinde nasıl koruyacaklar, onlara göre, küçük çocuklarla çalışırsam özellikle ilk öğretim düzeyinde öğretirim (M206).

Two of the participants said that raising information security awareness should be a school policy.

… Nowadays, everybody is using social media. Even the small children may have SNS account. For this reason, this could be proposed to school administration as an additional course in elementary schools (M102)…

... şimdi sosyal medyayı herkes kullanıyor. Küçücük çocukların bile SM de hesapları olabilir. Bu açıdan bence ilkokullarda bile bir ders olabilir, okullarda yönetime ders olarak önerilebilir (M102)...

We surveyed their (*elementary and secondary school students*) internet usage and found out that they have access to the internet from various platforms and have accounts in various social networking sites. However, they do not know what (*cyber*) ethics is. They do not know netiquette rules. They do not know what cyberbullying is. They have no idea about what they can do in case of a cyberbullying incidence. For this reason, the schools are supposed to take necessary measures (M201).

İlkokul ortaokul çağındaki öğrencilere anket yaptığımızda hepsi deli gibi bir çok farklı cihazdan internete ve sosyal medyaya erişimi var, ama etik nedir bilmiyorlar, internet kurallarını bilmiyorlar cyber bullying nedir bilmiyor, ya da bu durumda ne yapabileceklerini bilmiyorlar.Okullarda buna göre bazı düzenlemeler yapılmalı (M201).

Copyright and *academic integrity* were essential topics for pre-service teachers. Three interviewees mentioned that copyright was a critical issue on the course preparation process. They highlighted the importance of fair use exception.

We need to combine instruction and technology. During the instruction process, we should consider what we have learned in this course. We supposed to behave ethically so that our students can behave ethically (M110).

Öğretmenliği teknolojiyle birleştirmemiz gerekiyor. Bunu yaparken de öğrendiğimiz şeylere dikkat etmemiz gerekiyor. Bizim kendimizin etik bir şey ortaya çıkarması gerekiyor ki öğrenciler de etik davransınlar (M110).

> Particularly during the course preparation process, I will be careful about referencing and citation issues. Alternatively, sharing information through the net, I would teach them to be able to recognize correct or fraudulent contents and phishing sites (M208).

> *Öğretmenlik hayatımda, özellikle ders notu hazırlarken bir yerden aldığımda referans verme kısımları mesela. Ya da bilgi toplama, bunları öğrencilerle paylaşma, onların da çoğu seviyede internette doğru bilgiyi ayıklayabilmelerini sağlayabilmek olabilir. Mesela, maillere de bakmıştık, gerçek olmayan siteleri incelemiştik. Fake profil hoax içerik gibi (M208).*

> I think it is vital to give information about academic integrity in homework. I expect them to be able to express their opinions freely (M204).

> *Akademik dürüstlük kavramını öğrencilere aktarmanın çok önemli olduğunu düşünüyorum. Ödevde bile. Düşüncelerini düzgün bir şekilde dile getirebilmelerini isterim (M204).*

Five interviewees highlighted that academic integrity is an important issue when conducting teacher-student interaction. They also added that they could include honor code and code of ethics statements in their lessons.

The ethical use of ICT sources was also an essential issue for pre-service teachers. They stated that they would take security measures regularly in their professional lives. Creating a complicated password for the devices they use, and changing passwords regularly, and taking regular backup were the precautions they took for secure ICT use. One of the interviewees (M106) focused on the end user's responsibilities on the secure use of hardware devices.

> There are both mobile and desktop devices. They are being used everywhere, not limited to the schools. Every single person should be aware of the threats and must be security literate (M106).

Mobil cihazlar ve bilgisayarlar var, bütün işyerlerinde kullanılıyor, herkesin bu konularda dikkatli olması ve belirli bir seviyede bilgiye sahip olması gerek (M106).

Another contribution of the course was the rise in privacy concern of pre-service teachers both for them and for their prospective students. The participants were asked their preferences on the use of social networking sites (SNS) in their teaching professions. Majority of the students who have SNS accounts (13 of 18) stated that they would not create a connection with their students through their private SNS profiles. Those who do not have SNS accounts emphasized that teacher-student interaction through SNS was ethically problematic.

I have an (*SNS*) account right now; I will use it. However, I think teachers who take pictures with their students. I have teachers. I think that is wrong that teachers take and share pictures they took with their students, without consulting their family. I do not think I'm going to use it too much, even if it is permission. I do not find it very accurate to follow teachers on Facebook with their students (M108).

Şu an hesabım var, kullanırım. Ama öğrencileriyle fotoğraf çeken atan öğretmenleri yanlış buluyorum. Benim de öğretmen arkadaşlarım var. Bunun yanlış olduğunu düşünüyorum. Ailesine ve onun kendisine danışmadan buna hakkımızın olduğunu düşünmüyorum. İzni de olsa çok kullanacağımı düşünmüyorum. Öğretmenlerin öğrencileriyle facebookta takipleşmesini çok doğru bulmuyorum (M108).

On the other hand, the students highlighted the affordances of SNS and similar interaction tools on the Internet. Some of the students stated that they could use educational and limited online platforms like Moodle. Two interviewees shared their idea about creating a customized and limited SNS profile for the students. One of the interviewees pointed out the professional network affordance of these sites. She has started to log in those groups to develop a professional network.

> I can define another account to share course-related educational materials on Instagram because every student will be using. I do not consider to connect with students through a personal account (M102).
>
> *Instagramda ders materyaliyle ilgili etkinlik ve aktivitelerle, ilgili ayrı bir hesap açıp öğrencilerin onu takibi belki sağlanabilir, çünkü mutlaka herkes kullanıyor olacak, Kişisel bir hesap üzerinden bağlantı kurmayı düünmüyorum (M102).*

In summary, the pre-service teachers stated that they could use the contents they learned in their future life. Raise in the students' privacy concerns in SNS use influenced their internet related behaviors. These responses indicate that the course reflects positively to the students.

Table 4.36. *The list of topics in the sub-theme of Perceived Contribution to the Teaching Profession*

Phrase	Frequency
Integrate into Curriculum [a]	15
Employ the Honor Code	8
Ethical Use of Digital Sources	7
Suggest to School Administration	4
Use of SNSs in teaching process [b]	
No Interaction students through private SNS accounts	13
Special ways to communicate [c]	11

a: 5 interviewees stated that they would not want to be a teacher; the responses presented in the first four rows were out of 18 participants. On the other hand, the five interviewees, who said to have different career plans rather than being a teacher, confirm that the course contributes their plans as well.
b: 4 interviewees stated that they did not have an SNS account. The responses presented in the two rows below were out of 19 participants.
c: These special ways include course management sites, such as Moodle, limited SNS accounts, or special purpose groups, pages

Five interviewees stated that they do not plan to be a teacher in future. However, they included that the topics they learned in the course were necessary for their future plans. Particularly information security issues and code of ethics were

important gains they got from the course. A summary of related responses is presented in Table 4.36.

4.4.5. Direct Effect to Daily Lives of the Students

Students influence their families or friends. One of the interviewees said that she was informing her parents about the risks of sharenting and oversharing. By doing so, she stated that she could raise her family's information security awareness. Another student said that she warned her friends who shared their ticket on an SNS with a QR code on it.

> Recently, when I was applying for … my TC identity code was asked. I have concerned submitting it. Your warning about information sharing has influenced me. TC id no is our unique identity. We have to be careful about it. For example, I have some friends who share their tickets including QR codes on it. If they are close, I warn them (M101).

> *Geçenlerde web üzerindeki bir … başvurusunda TC mi (*TC Kimlik NO*) istediğini gördüm, tereddüt ettim, formu göndersem mi diye. Bilgi paylaşma konusundaki uyarılarınız çok yer etti. TC bizim unique idenditymiz, paylaşırken dikkatli olmamız gerek. Mesela yine Instagramda QR kodlu bilet paylaşan arkadaşlarım var, yakınsa uyarıyorum. (M101).*

> … Oversharing and sharenting for example. These are the issues we always meet in our daily lives. I think the subjects in the course provided more awareness (*about these issues*). I am trying to prevent my family from sharing the photos of the children in the family. Because I realized that it bothers us too. Passive digital footprints are created before the child grows (M208).

> *… Mesela, oversharing, sharenting. Bunlar hep günlük hayatta karşılaştığımız şeyler. Dersteki konuların daha çok bilinçlenmemizi sağladığını düşünüyorum. Ailemdekilere çocuklarının fotoğraflarını*

paylaştırmamaya çalışıyorum. Çünkü farkettim ki bizi de rahatsız ediyor artık. Daha çocuk büyümeden pasif digital footprint yaratılıyor (M208).

The course affected the students' academic lives. Two students stated they have benefitted from the course contents in their other course projects, and they started a project aiming at informing the elementary school students by using the information they learned in this course.

Two students of the first implementation stated that they were more confident in a course they enrolled in the spring semester. The term "Creative Commons" is explained in that lesson, and they had a chance to contribute to the lecture.

The interviewees stated that they could recognize and understand the contents of acceptable use policies. One of the participants said that she did not read the terms of service statements before the course. The students said that they felt more self-confident when they download a file or fill a form since they felt they were aware of the privacy issues.

4.4.6. The Exam Results

The detailed information about the first and the second midterms and final examinations for the first and second implementations are presented in the sections 4.1.3.2 and 4.1.3.4 respectively. In this section frequency analyses of correct answers are interpreted.

4.4.6.1. The First Mid-Term Exam in the First Implementation

There were 21 questions in the first mid-term exam. When the frequency analysis of correct answers to the first mid-term exam was conducted, it was seen that of 14 of 21 questions of the test were answered correctly by more than 30 of the 40 students. On the other hand, the question which asked the abbreviation of Information Security Management System Standards (ISO27000) was answered wrong by nearly half of the students. The students confused that with the Internet Law 5651. However, the correct response rate to the security-related questions, such as malware, phishing, or malicious human threat was higher than 75%. The highest grade was 105, and three

students got it. The average for the exam was 85.13. The description of the questions and correct answer rates are presented in Table 4.37.

Table 4.37. *Question Descriptions and Correct Answer Rates of the First Mid-Term Exam of the First Implementation*

Description of the question	Nb. of Correct Answers	Percent
IT Resources Use Policy of the University – General Provisions	38	95%
IT Resources Use Policy of the University – ULAKBIM	25	63%
MoNE Information Security Directive	40	100%
5651 Internet Law	37	93%
Information Security Management System Standards	17	43%
Information Security Objectives – CIA Triad	40	100%
Information Security Objectives – Confidentiality	22	55%
Information Security Objectives – Integrity	35	88%
Information Security Principles – Absolute Security	38	95%
Hacker Types – White Hat Hacker	21	53%
Hacker Types – Malicious Insider	27	68%
Security Threats – Vulnerability	34	85%
End Users – Definition	33	83%
End Users – Information Security Awareness	39	98%
Malware – Definition	32	80%
Malware – Trojan	30	75%
Digital Information Assets	34	85%
Digital Identity – Password Security	31	78%
Digital Identity – Phishing Mail	38	95%
Digital Identity – User Generated Identity	37	93%
Mobile Security – Definition	29	73%
General Average		81%

4.4.6.2. The Second Mid-Term Exam in the First Implementation

In the second exam, 26 questions were asked to the students. Nineteen questions were test type, and seven questions were matching type questions. Analyzing the frequencies of correct answers, it was seen that, 12 of the 19 test questions (including the bonus question), and five of seven matching questions were answered

true by the majority of the students. Whereas the nine questions were correctly answered by the half or minority of the students. The average correct answer rate of the questions was 84%. The description of the questions and correct answer rates are presented in Table 4.38.

Table 4.38. *Question Descriptions and Correct Answer Rates of the Second Mid-Term Exam of the First Implementation*

Description of the question	Nb. of Correct Answers	Percent
Cyberethics – Definition	36	90%
Cyberethics – Ten Commandments	39	98%
Cyberethics – Controversial Issues	12	30%
Code of Ethics – Definition	28	70%
Code of Ethics – Example	24	60%
Intellectual Property – Definition	33	83%
Copyright – Duration	9	23%
Fair Use – Example	37	93%
Copyright – DMCA	16	40%
Anti-Copyright Act – Definition	38	95%
Anti-Copyright Act – Creative Commons	17	43%
Patent – Duration	15	38%
Privacy – NORA	21	53%
Cheating – CoHE Regulations	40	100%
Cheating – Reasons	20	50%
Academic Dishonesty – Example	37	93%
Plagiarism – Reason	18	45%
Plagiarism – Example	40	100%
Mustafa Akgül	17	68%
7 Matching Questions – 9 Elements of Digital Citizenship (average)	28	70%
General Average		67%

4.4.6.3. The Final Exam in the First Implementation

There were 30 questions 15 of which were test, and the rest was matching questions. Analyzing the frequencies of correct answers, it was seen that, 12 questions of the 15 test questions and all matching questions were correctly answered by the majority of the students. Whereas the three questions were answered correctly by half of the students. The average correct answer rate of the questions was 84%. The description of the questions and correct answer rates are presented in Table 4.39.

Table 4.39. *Question Descriptions and Correct Answer Rates of the Final Exam of the First Implementation*

Description of the question		Nb. of Correct Answers	Percent
Information Security Management System Standards		32	80%
Hacker Types – White Hat Hacker		29	73%
Cyberethics – Controversial issues of Ten Commandments		19	48%
Copyright – Duration		20	50%
Patent – Duration		33	83%
Privacy – NORA		25	63%
Cheating – Reasons		24	60%
Copyright – DMCA		35	88%
Plagiarism – Word-to-word Copying		19	48%
Cyberbullying – Definition		36	90%
Nomophobia – Definition		39	98%
Oversharing – Definition		38	95%
Clickbait and Hoax – Differences		37	93%
Sharenting – Example		40	100%
Sharenting –Risks		39	98%
Definition – Matching Questions			
A.	Information security	37	93%
B.	Cybersafety	34	85%
C.	Cyberethics	37	93%
D.	Vulnerability	39	98%
E.	Risk	29	73%
F.	Confidentiality	34	85%
G.	Sharenting	37	93%
H.	Integrity	38	95%
I.	Cheating	37	93%
J.	Availability	36	90%
K.	Risk	40	100%
L.	Digital Identity	40	100%
M.	Hacktivists	30	75%
N.	Patent Troll	39	98%
O.	End user	36	90%
Average			84%

4.4.6.4. The First Mid-Term Exam in the Second Implementation

The detailed information of the first midterm in the second implementation is presented in section 4.1.3.4. When the frequency analysis of correct answers was conducted it was seen that, 17 of the 20 test questions and seven of 10 matching questions were answered correctly by the majority of the students (15 and more students in 21).

Whereas the two questions were correctly answered by the minority of the students. One of the questions was related to the Code of Ethics of the university which was briefly introduced in the lecture. It was given as reading material. Those who read the Code of Ethics were able to answer correctly. The other question, correctly answered by five students, was one of the matching questions about the elements of digital citizenship. The majority of the students confused the terms of digital law and digital responsibilities.

On the other hand, correct answer rate for the questions about copyright, fair use, academic dishonesty, and cyberethics indicate that the students understood these concepts. The average correct answer rate of the questions was 81.1%. The general grade average was 80.1. The highest grade among the students was 98. One student got the highest grade. Seven students got 90 and higher grade. The description of the questions and correct answer rates are presented in Table 4.40.

Table 4.40. *Question Descriptions and Correct Answer Rates of the First Mid-Term Exam in the Second Implementation*

Description of the question	Number of Correct Answers	Percent
IT Resources Use Policy of the University – General Provisions	19	90.5%
MoNE Information Security Directive	21	100.0%
Cyberethics – Definition	20	95.2%
Cyberethics – Ten Commandments	19	90.5%
Code of Ethics – Example	7	33.3%
Intellectual Property – Definition	17	81.0%
Cyberethics – Controversial Issues of Ten Commandments	16	76.2%
Acceptable Use Policy – Definition	15	71.4%
Copyright – Duration	16	76.2%
Anti-Copyright Act – Definition	20	95.2%
Fair Use – Example	20	95.2%
Cheating – CoHE Regulations	21	100.0%
IT Resources Use Policy of the University – Definitions	13	61.9%
5651 Internet Law	17	81.0%
Copyright – DMCA	17	81.0%
Anti-Copyright Act – Creative Commons	12	57.1%
Cheating – Reasons	15	71.4%
Academic Dishonesty – Example	18	85.7%
Plagiarism – Example	20	95.2%
Digital Footprint – Permanence	16	76.2%
10 Matching Questions – 9 Elements of Digital Citizenship Concepts (average)	16	77.1%
General Average		81.1%

4.4.6.5. Second Mid-Term Exam in the Second Implementation

The detailed information of the second midterm in the second implementation is presented in Section 4.1.3.4. When the frequency analysis of correct answers was conducted it was seen that, almost all questions (19 of 20) were answered correctly by the majority of the students (14 and more students in 17). The average correct answer rate of the questions was 90.2%. The general grade average was 98.89 out of 110. After the make-up results included the average decreased 95.71. The highest grade among

the students was 110. One student got the highest grade. Nine students got 100 and higher grade. The description of the questions and correct answer rates are presented in Table 4.41.

Table 4.41. *Question Descriptions and Correct Answer Rates of the Second Mid-Term Exam in the Second Implementation*

Description of the question	Number of Correct Answers	Percent
Cybersafety – Definition	14	82%
Privacy – Definition	14	82%
PII – Definition	14	82%
PII – Example	17	100%
Privacy – NORA	15	88%
Clickbait and Hoax – Differences	15	88%
Sharenting – Example	14	82%
Sharenting – Risks	17	100%
Oversharing – Definition	15	88%
Cyberbullying – Examples	16	94%
Cyberbullying – Definition	17	100%
Cyberbullying – Victim characteristics	16	94%
Safety Issues of SNS – Example	16	94%
Freedom of Speech – Digital Citizenship correspondence	10	59%
Freedom of Speech – Definition	16	94%
Symbolic Speech – Example	16	94%
Addiction – Digital Citizenship correspondence	17	100%
Addiction – Definition	17	100%
Computer addiction – Definition	17	100%
Nomophobia – Definition	17	100%
Bonus Question	12	71%
General Average		90.2%

4.4.6.6. Final Exam in the Second Implementation

The detailed information about the final exam in the second implementation is presented in section 4.1.3.4. When the frequency analysis of correct answers was conducted, it was seen that 12 of the 26 questions, were answered correctly by the

majority of the students (15 and more students). However, five questions were correctly answered by a minority (less than 10) of the students. The average correct answer rate of the questions was 70.6%. The description of the questions and correct answer rates are presented in Table 4.42.

Table 4.42. *Question Descriptions and Correct Answer Rates of the Final Exam of the Second Implementation*

Description of the question	Nb. of Correct Answers	Percent
5651 Internet Law – Definitions	13	65%
Information Security Objectives – Integrity	15	75%
Information Security Principles – Layers of Defenses	15	75%
Digital Identity – Password Security	18	90%
End Users – Description	18	90%
Hacker Types – White Hat Hacker	14	70%
Digital Identity – Phishing Mail	13	65%
End Users – Information Security Awareness	20	100%
Information Security Objectives – Confidentiality	8	40%
Cyberbullying – Examples	14	70%
Security Threats – Vulnerability	18	90%
Mobile Security – Definition	8	40%
Malware – Trojan	18	90%
Freedom of Speech – Censorship	20	100%
Attack types – Nation-state attack	14	70%
Privacy of SNSs – Student – Teacher Interaction	18	90%
Cyberbullying – Proper action after an incidence	20	100%
Addiction – Ways to handle	8	40%
Privacy – PII	7	35%
Sources of Digital Footprint	18	90%
Cyberethics – Definition	13	65%
Copyright – Fair Use Example	8	40%
Anti-Copyright Act – Creative Commons	19	95%
Academic Dishonesty – Example	14	70%
Plagiarism Types	13	65%
Code of Ethics of the Course	3	15%
General Average		70.6%

4.4.7. Summary of the Theme

"*Potential contributions*" theme mainly answered the third research question;

> *"How do pre-service teachers perceive the contribution of the course on their information security awareness and cyberethics sensitivity?"*

The major issue emerged potential contributions theme is that; the course affected the students in various ways. The most common effect was their behaviors on secure ICT use. The students emphasized their changed behaviors and raised awareness both in the interviews and during the lecture sessions.

Table 4.43. *Summary of Findings for Research Question 3*

The possible facilitating and challenging factors for the design, development, and implementation process of the course.		
Newly learned	• Almost all of the topics, • Terminology, • Concepts in detail • Copyright related details	• Fraudulent content • Social Media privacy • Hacker and attack types
Correcting misconception	• Self-plagiarism • Privacy settings in SNSs	• The permanence of Digital footprint • Https
Raised awareness	• Raise in computer literacy • Change in password change frequency • Secure surfing • Phishing • Hate Speech	• Copyright and DMCA Issues • AUP and ToS awareness • Changed SNS habits • Cyberbullying • Fraudulent content

Perceived contribution to the teaching profession	• Special Profile or System for online interaction
	• Knowledge Transfer
	  ○ Integrate into Curriculum
	  ○ Suggest of K12 Schools administrations
		• Aware ICT Use
		  ○ Academic Integrity
		  ○ Free Speech
		  ○ Self-Privacy Concern
		  ○ Students' privacy concern

Direct effect on daily life	• Benefit in another course • Familiarity on Copyright issues and License Types • Secure surfing (https) • SNSs Safety and Preserving PII • Self-confidence in a cyber-bullying incidence	• Became alert in a phishing attempt • Change in password management preferences • AUP and ToS awareness • Influence on family and friends

The students' in-class discussion participations have also demonstrated this change. For example, in the sixth session of the first implementation, the security of mobile devices was the major topic. The instructor explained the application security and the permissions which the applications asked during the installation. On the discussion session, the second hour of the lecture, the instructor realized that most of the students checked his or her applications and which permissions were given during the installation. A summary of the findings of this theme is presented in Table 4.43.

4.5. Summary of the Chapter

During the first implementation, the researcher utilized several resources, printed or electronic books, journal articles, e-zine and blog sites in order to develop an explicit, detailed course content throughout the semester. The content sequence has a crucial value in the semester-long course design. During the weekly course implementations, the researcher utilized several course delivery and interaction methods. She provided reading materials, workbooks, guidelines, and additional video links for the students. The recommended reading materials were available from the university's library and the Internet. She employed forum discussions and managed in-class discussion sessions. All these efforts were based on the assumption that students would be sufficiently involved and willing to contribute. On the other hand, the students' contribution was less than expected. Besides, their forum participations were increased just after they noticed that it would affect their participation grades.

Based on the experiences throughout the first semester, the second implementation was designed and developed. The summary of the issues encountered in the first implementation is presented in Table 4.44.

Table 4.44. *The summary of the issues encountered in the first implementation*

Issues	Interventions
Starting the course with Information Security topics caused the students to feel more anxious about the course	• The content sequence is changed so that the more recognizable topics were located at the beginning of the semester.
Students seemed to be they did not prefer reading	• More detailed lecture notes were prepared for students • The recommended reading materials were introduced in the classroom.
Forum participation was lower than expected.	• Predetermining forum threads and creating them hidden makes it possible to use the online component of the course more efficiently. • The grading policy and value of *participation* are explained in more detail. • The discussion session was included in the contents of the current week's forum discussion contents.
It was difficult to memorize the names of students, especially for low-participating ones	• In the introduction session, in order to get to know the students, the researcher asked their names and their expectancy from the course. • In the following few weeks in the discussion forums, she asked their names before their speech.
Inadequacy of English was another problem related to the efficiency of the course.	• For this reason, in some cases, critical information is explained in Turkish.

During the second implementation, the course outline has been ripened. Methods of instruction were the same as the previous semester. However, new discussion forum topics were launched. At the end of the second implementation, new issues and interventions and new decisions have emerged. The interviewees, furthermore, suggested different instructional interventions. All collected information is evaluated, and a guideline was formed. Based on the experiences throughout the second semester, the encountered issues and related measures are presented in Table 4.45.

Table 4.45. *The summary of the issues encountered in the second implementation*

Issues	Interventions
Forum participation is not at the expected level	• Different forum topics have launched. Only one main topic could be defined. • Notification settings of the system could be checked. • The effect of forum participation could be explained more explicitly.
Only some of the students fully participated in class discussions.	• The instructor announced a 3-row rule and prohibited the sparse sitting.
The extended lecture notes were launched a week after the lesson.	• The students expect to be prepared for the lecture hour. For this reason, it is better to be launched before lecture hour.
Deficiency of audiovisual materials	• Because of the computer crash experienced in the first implementation, the researcher did not include any video in the second implementation. Instead, she included such material after the lecture hour. However, it was found to be a weakness for the course according to the students.
Memorizing the terminology is a concern of some of the students.	• A glossary of terms could be provided to the students. Besides, in-class activities and gamified activities could be employed.
Inadequacy of English was another problem related to the efficiency of the course.	• For this reason, in some cases, critical information is explained in Turkish.

4.6. Researcher's Opinion

It was an informative experience to design, develop, and implement a course, some details of which, such as various topics within the content and methods of instruction, were not known (by the researcher) and classroom experience was not possessed before. The topics covered throughout the semester have contributed to the researcher professionally. Not only an experienced employee in the computer center of a university but also as a digital citizen, this research contributed to the researcher's awareness of her rights and responsibilities. Working knowledge of information security is a requirement of the researcher's profession. On the other hand, she did not have sufficient background on other topics such as copyright, cyberbullying and free speech which are outside of her professional interest. This study has raised her level of knowledge on these issues.

As an outcome of this study, the researcher has acquired significant experience in design-based research. While developing a course, regardless of how much prior research about the learners has been done, one should always be prepared to encounter unexpected and new elements. The contents of the subject matter should comply with the current conditions. Especially, for a course whose content is continuously evolving and changing day by day, it is seen that design-based research is an important research method.

CHAPTER 5.

DISCUSSION AND CONCLUSION

In this chapter, the discussion and conclusion of the study based on the findings are presented. The organization of the chapter is based on the three main research questions of the study. Each section includes the principal results of the study. The chapter concludes with the presentation of implications for practice and practitioners in course development, the researchers working on design-based research, and information security and cyberethics tutoring and training practitioners.

The major purpose of this study was to design, develop and implement a course aiming at raising pre-service teachers' information security awareness and cyberethics sensitivity. Design-based research methods guided the study. In line within this purpose, the researcher conducted a needs analysis study and determined the broad content pool. In the next phase of the study, the researcher developed a detailed course syllabus, including the course objectives, content sequence, and other related components.

During the needs analysis and development of course phases, several sources of information were utilized. Review of recent survey studies, security reports, and expert interviews were main sources of information during the preparation of the content pool.

During the iterative implementation phases, two implementations were conducted in two successive semesters. The researcher developed the course, designed weekly lectures, moderated discussion forums and in-class discussions, prepared and evaluated the mid-term and final exams. During all these steps, designer reflections and field notes were taken, and these guided the design of the lectures of the successive weeks. Detailed information about weekly lectures is presented in Section 4.1.2.2.

5.1. Key Issues about the Design and Development Period

The issues encountered in the design and development period of the study are grouped as (i) content, (ii) learner, and (iii) instruction related. The findings gathered from the designer reflections, field notes, and the interviews are presented in the previous chapter. In this section, the findings addressed in the previous chapter were discussed.

5.1.1. Key Issues about the Content

There were several issues the researcher needed to consider. Since there was no ready-made course content for the end users in the areas of IT security and cybersafety, preparing the course contents was one of the significant outcomes of this study. In the content preparation process, multidisciplinary nature of the course and determination of the technical levels of the contents were critical concerns. It was encountered during the implementations that the content sequence has an essential effect on the students' attitude toward the course.

5.1.1.1. Multidisciplinary Nature of the Course.

Information security is a multidisciplinary topic (Wood, 2004). Merkow and Breithaupt (2014), describe the multidisciplinary nature of information security as follows:

> *A multidisciplinary approach describes the breadth of people's knowledge and experience across a wide variety of interests—scientific, liberal arts, business, communications, and so on. Those who can maintain a wide view of the world (or a business situation) tend to excel when working in information security (p.8).*

Besides, the contents of this course include cyberethics and cybersafety terms, such as freedom of speech or addiction which refer to different disciplines, such as law and psychology. Information security awareness topics have technical aspects such as protection measures and accessibility. On the other hand, the freedom of speech, a cyberethics issue, is related to law, and as a course designer, the researcher was required to know related constitutional and legal statutes.

In addition to the requirement of mastering the regulations in these topics, determining how deep these issues would be given to the students in the course to be prepared was also a matter of consideration of the researcher. Determining the level of the contents is a natural concern for designing multidisciplinary courses. Stahl, Moira, and Peter (2006) highlighted the possible problems of developing a multidisciplinary course in the area of forensic computing. They underlined that it was essential to decide the critical and necessary points of each disciplinary area. In this research, the researcher decided the content of each topic at the introductory level as well as she took the students' future profession into consideration.

Addiction is a psychology-related topic within the context of cybersafety. Because the researcher's background about psychology is not at the expert level, the reasons and the possible effects of computer and internet addiction were included in the course at an introductory level. Another example of multidisciplinary content is the copyright and licensed software issues. The related course content included legal statutes.

Since this course addresses critical information from different disciplines, for some lectures, a guest instructor from a different a discipline could be invited to the lecture to give a seminar and hold a question-answer session. A guest instructor may increase the students' interest in that topic. Since the guest instructor is an expert, this raises the quality of the lecture. On the other hand, if these sessions are not a part of grading, the students might lose attention.

5.1.1.2. Depth and Breadth of the Course Contents

In the course, the role of the learners affects the course design. Deciding the depth and breadth of the contents, in other words, to what extent the course topics would be explained to the students is a critical point to concern.

Especially, for the information security topics, the technical level of the educational material was quite high. Majority of the existing resources were written for information system (IS) professionals with the assumption of higher-level technical knowledge and responsibility compared to end users'. The potential readers were IS professionals or managers. It was found to be quite challenging to simplify the

language and technical level of the contents to the end users' level. When explaining the crucial facts about information security, at the beginning of the corresponding lecture session, the researcher simplified the topics and omitted some of the topics which required a high-level digital literacy. For example; in the first session of the information security lectures; the researcher made use of the first chapter of the book "Computer Security Literacy (Jacobson & Idziorek, 2016)." However, some of the terms used in the book, such as the explanation of "*vulnerability types*" and "*risk assessment*" are not included in the course. Because these topics were addressed at system designers and information security professionals, respectively.

Similarly, the subtopics of intellectual property included (i) definitions, (ii) history of copyright, (iii) first sale doctrine, (iv) fair use issues, (v) DMCA, (vi) trademark, and (vii) duration of copyright and trademark. During the implementations, all topics related to intellectual property were introduced to the students such as copyleft movement and related issues. However, the first sale doctrine was a technical issue for copyright owners. For this reason, it was not included in the outline of the second implementation.

To summarize, during the design and development of a course, the instructor should consider the learners' needs and background. The topics should be such that future use them in students' career is evident, and therefore students would not question the necessity of covering that particular topic.

5.1.1.3. Content Sequence of the Course

One of the considerable challenges was to determine the content sequence at the beginning of the study, the pre-implementation phase. The content sequence has a critical role in designing a course syllabus (Hess & Whittington, 2003). The main objective of the course was to raise the students' information security awareness. For this reason, the focus was on cybersecurity-related topics. The contents are sequenced accordingly (Leshin, Pollock, & Reigeluth, 1992). As a result, the course is designed in the first implementation with the content sequence presented in Appendix F.

Once a course outline is set, some of the students of the first implementation reported that they had difficulty in grasping the course content. Cybersecurity topics

with detailed computer related terms were introduced to students at the beginning of the semester. Since the students have found cybersecurity-related topics to be difficult, at the beginning of the semester, their concern about the course continued throughout the semester.

For this reason, the content sequence has been radically changed in the second implementation. The objectives of the course and the focus on cybersecurity remained. The researcher decided to explain cybersecurity-related topics throughout the semester and gradually increase the technical level of the course. The students of the second implementation felt more confident compared to the students of the former implementation. It was seen both in the responses of the interviewees and the researchers' field notes.

Since the content sequence is critical, the instructor of such a course must be prepared to modify the coverage according to the learners' background. When the learning curve is steep at the beginning, not only this intimidates the students, but also re-explaining the topics causes time loss.

5.1.2. Key Issues about the Learners

The researcher found critical issues about the learners which affected the implementation processes. Their prior knowledge, motivation to take this course, their major fields, and their future plans affected their attitudes toward this course.

5.1.2.1. Students' Prior Knowledge and Their Behaviors toward the Course

Regarding the learner related issues, it is found that the diversity of learner background could have a significant impact on instruction and student learning. Whatever their fields are, these students are *digital natives* (Prensky, 2001). Prensky (2001) describes the new generation as they have been grown up into new digital technologies, such as cell phone, television, computer and video games, and similar new and fast communication tools. He defines digital natives as "*native speakers of the digital language of computers, video games and the Internet* (p: 2)."

The students of both implementations were, like any digital native person, familiar with digital technologies such as SNSs, mobile devices, and applications. As

a result, their contribution to lecture and discussion was at the highest level during the mobile security and SNS privacy related lectures.

Their familiarity with the internet and mobile technologies might cause some misconceptions. It was realized that the students knew some of the topics in the wrong way or they had deficient information. The primary issue they have come to recognize in the course was about the measures for protecting digital reputation. Since they are active SNS users and possessing mobile devices, generally, giving attention to privacy issues about SNS and mobile applications have critical value. Yavanoğlu and his company (2012) concluded the risks of SNS use among K12 level students and highlighted that end users are more vulnerable for phishing attacks, fraudulent contents, and malicious SNS applications. They recommended protection measures both for the users, their parents, and their teachers. Briefly, they recommend to protect PII, not to share exact personal information, be careful about fraudulent contents. The focus of cybersecurity and cybersafety issues of the course included these measures.

During the two implementations, in the lecture sessions, the researcher encountered that the students' attitudes during in-class discussions or forum participation varied based on their major fields. The computer literacy level of CEIT students was higher than that of the other students of faculty of education. It was the natural result of CEIT curriculum (CEIT, 2018). Regarding CEIT students, their level in the program affects their background knowledge.

In the first implementation, CEIT students were more involved in class activities during cybersecurity-related topics which were covered at the beginning of the semester. On the other hand, in further weeks, while cyberethics or privacy issues of SNSs were explained, participation in class discussions were increased through the contributions of the students from other fields.

Students' prior knowledge and their familiarity with the concepts positively affected their participation. For this reason, as it was mentioned in the previous section, 5.1.1, the content sequence and the outline were designed accordingly. As it was mentioned in Section 4.4.1, the interviewees who said that they knew the topics before the course, added that they had a chance to learn them in more detail. Furthermore,

interview results indicated that there might be some misconception which was corrected as a result of taking the course.

Not only the students' course-related prior knowledge but also their English skills affected their contribution. This course depends on discussion and reading. Their participation in the lecture and discussion session was affected by their English level. The fact that the medium of instruction is English affects the participation of students who are not native speakers of this language.

As a result, to eliminate the difficulties regarding the diversity of backgrounds, some strategies could be implemented. One strategy could be separating groups of students and offering customized courses to each separate audience. On the contrary, different backgrounds could also be an advantage if the students could be made to work in groups for group projects.

Even though the students are coming from different majors, they still have a common background consisting of a certain level of computer literacy, typical habits of SNSs use, and the prospect of using acquired awareness, knowledge, and skills in their careers. For example, teachers are expected to be role models for their future students, regarding their online presence. On the other hand, if the general public is considered, most of these elements cannot be assumed. Most importantly, not all the topics covered in this course will be of interest to the general public. For example, academic integrity issues or fair use of intellectual properties are directly related to the educational context. On the other hand, core issues regarding cyberethics, cybersafety, and cybersecurity are critical to all end users and they might receive instruction through seminars or conferences as well as web-based guides.

For other professions, minor arrangements could be made to the content sequence in-line with the profession. Some of the subjects could be brought forefront whereas some others could be reduced or eliminated. For example, for engineering students, while explaining the intellectual property topic, patent-related issues are more critical rather than fair use. One size fits all approach not suitable in this case, and the whole course design should be revised by collaborating with the professionals of that field.

5.1.2.2. Students' Career Plans

The students' approach to the course varied according to their major fields. It was also found out from the interview responses. The main objective of this course was not only to raise their information security awareness and cyberethics sensitivity but also to provide guidance for them in their future teaching profession. However, CEIT students, in general, do not have a career plan about being a teacher. Sevim, İslim, and Kaplan Akıllı (2016) confirmed that after graduation, CEIT students are more inclined to choose to different professions rather than being teachers. They feel themselves outside of the faculty of education. The interviews did not aim at identifying CEIT students' career plans, but this observation should be taken into account while evaluating some oppositely different responses of CEIT students to interview questions.

Besides, this course is designed at the introductory level for end users who are thought to have lower computer literacy. As a result, the contents in this course did not satisfy CEIT students' expectations. The researcher concluded that the accurate target group of this course is non-CEIT pre-service teachers. This course can be given to the first year CEIT students as an introductory course. After passing this course, they can take an advanced version of this course including more technical details about information security, cyberethics and cybersecurity details of coding, managing IT services, and similar security issues for IT employees.

5.1.2.3. Students' Approach to the Course

The students took this course as an elective course. Babad (2001), highlights that the course difficulty and high-grade expectations are the main predictors of course selection. In the first implementation, the students' concern was about grading policy and whether they could get a high grade. In the first session of both implementations, and during the registration period, some of the students stated their computer related concerns. This was also an indicator of their grade related concerns.

The students, at the end of the semester, confirmed that the course would contribute their teaching careers; however, in the beginning, their concerns about course difficulty and grade policy had priority. This might be due to the course is being

an elective course. Their attitudes toward must courses are different; when they face a heavy overall workload, they prefer to focus on a must course instead of an elective course. Their interview results also confirm that in case of a homework load, they could not concentrate on this course.

Students' attitudes toward their courses may depend on several factors. J. M. Curran and Rosen (2006) state that the physical environment, subject, and presentation of the course and the personality of the teacher significantly affect students' attitudes towards their courses. Particularly, teachers' acknowledgment on the students' participation has a positive impact on the student's contribution to the course.

In this course, their participation in both class and forum discussions were appreciated and encouraged by the researcher. Their participation in class discussions depended on how interested they were about the subject.

5.1.3. Key Issues about the Instruction

The key issues which the researcher encountered about the instruction are grouped as follows: (i) key issues about instructional materials, (ii) suggestions about instructional design. It was a blended course, including both face to face lecture with an online environment. During the face to face lectures, in the first hour, the topics of the week were lectured. In the second lecture hour in class discussions were made. The online environment included recommended links and forum discussions.

The researcher designed weekly presentations, moderated the discussion forums, prepared and evaluated the midterm and final exams. At the beginning of the first implementation, the course outline was designed on the assumption that students would read the reading materials and be prepared in the lecture session. In this case, discussions and lecture participation would be more effective. For this reason, the researcher uploaded reading materials about the topic of the current week to the online environment of the course. However, the majority of the students reported that they did not prefer to read them. As a result, the researcher prepared extended lecture notes and made them available to the students in addition to reading assignments for the second implementation.

Owusu-Acheaw and Larson (2014) reported that reading habit has a direct influence on academic performance. However, the majority of students do not prefer reading. Owusu-Acheaw and Larson (2014) added that the students' reading motivation was limited to passing examinations. On the other hand, they advised the lecturers not to provide handouts and encourage the students to read.

The primary objective of this course was to raise the students' information security awareness and cyberethics sensitivity. For this reason, the primary strategy was to increase their familiarity with the concepts. There may be several reasons for not reading the reading assignments. Since the students who said they have read were only from FLE department level of English of the students might be the reason.

The researcher would have preferred if the students had read the reading assignments and attended the lectures with prior preparation. However, since they declared in different ways that they do not read, or did not want to, the researcher prepared a handout for each week. The handouts included extensive information about the corresponding topic in the second implementation. They were read by almost all of the students in the second implementation. Furthermore, the detailed and extensive information in these handouts were found to be useful for exam preparation.

Kruger (2003) suggested three methods for cyberethics training for teachers which are (i) teaching by example, (ii) including cyberethics into assignments, and (iii) seeking online cyberethics resources. The examples were part of the discussion session. Not only cyberethics related issues, but also cybersafety and cybersecurity-related topics were clarified with real-life experiences and observations as well.

During the instruction, in-class discussions were found to be useful. The students confirmed that discussion forums were useful to understand the topics covered in the lectures. Particularly cyberethics discussions presented different points of view and controversial issues on a specific topic. They include in the interviews that these affordances were favorable among the students.

To be able to think and write about information security and cyberethics was one of the objectives of the course. To develop this skill, discussion forums have been created. Delaney, Kummer, and Singh (2019) stated that an online forum is a useful

part of the learning process. Forum responses indicate that the students have developed their cyberethics understanding.

The researcher realized that the students were trying to memorize the subjects of the lesson, and therefore they confused the subjects even more. At the last session of each implementation, the researcher made a general review session and tried to clear possible misconceptions.

Some topics confuse students. Confusion between hoax and clickbait, or the security standards and the internet law can be mentioned. The researcher has to take these confusing topics into account.

The major difference between the two implementations was the increased support of the native language. In both implementations, the medium of instruction was English, and none of the students in the class were native English speakers. The discussion sessions were in Turkish. In the second implementation, the researcher explained the course contents in Turkish after lecture sessions. In both implementations, the language of the course materials and online activities were English. The interviewees from the first implementation complained about the language of instruction. Oppositely, Turkish explanation and lecturing was a favorite detail of the course for the second implementation interviewees.

The terms of information security presented a new terminology for non-CEIT students. For this reason, this new terminology should be presented to the students in more detail. In this step, a *glossary of terms* would be included as course material at the beginning of the semester. The researcher provided extended reading notes in the second implementation. It would be more beneficial if these reading notes were provided to students before the session.

To summarize, a blended course was designed with a lecture session and synchronous/asynchronous discussion elements. This course could not be given only through face to face lectures. To be able to develop knowledge and writing skills about information security and cyberethics is one of the objectives of the course. Blended format is more appealing to the students. Maintaining computer interaction opens a venue for the students to interact with the wealth of information on the internet.

Besides in the future implementations of the course, games, online quizzes, more audio-visual learning materials could easily be incorporated to the course.

5.2. Factors that Affected the Implementation

Several factors affected the design, development and implementation periods of the course. According to the interview results, the students underlined different factors that facilitate or challenges them on course-related activities.

5.2.1. Facilitating Factors

Daily life correspondence is the leading facilitating factor both for the students and the instructor during the implementations. The researcher was able to relate the topics taught in the lectures to recent news or the students' daily routines. At the discussion session, the students could give a trendy example of the topic of the current week.

Students being digital natives (Prensky, 2001) was also a facilitating factor for the instructor. The topics taught in the lecture immediately affected students' behaviors during their ICT use or online presence.

The instruction style, discussion sessions and the instructor's detailed explanations, supply of different examples and descriptions from different sources were the details about the course which the students were in favor of.

5.2.1.1. Daily Life Correspondence of the Course

Brouwer and Korthagen (2005) highlight that daily life integration in teacher training institution has a recognizable impact on their professional experiences. The students stated that this course had an impact not only on their daily life experiences but also it raised their awareness on the issues which will help them in their teaching experiences.

There is a strong need for raising information security awareness. During the design phase of the study, it was a motivating factor of the study, both for the researcher and the experts who contributed to this study with their suggestions and experiences. Another critical point was the recent change in the teacher training

curriculum in Turkey. During the first implementation, CoHE (2017) published a new curriculum for teacher training institutions and included a computer security and cyberethics course for CEIT students.

Since the use of the Internet and social media tools have vastly increased, secure, safe and ethical use of the Internet became more critical for privacy and safety of the individuals. The institutions in different disciplines are concerned about their employees' information security awareness and cyberethics sensitivity. The focus of attention may vary. With the rapid spread of ICT technologies in our lives, secure and ethical use of social media gained attention. For example ethical behaviors of nurses (Lachman, 2013) or ethical issues of teaching with social media (Henderson et al., 2014) categorically focus on privacy issues of patients and students respectively. Copyright and license issues are the ethical foci of business settings (Stahl, 2009).

Pre-service teachers' education about information security and cyberethics is a valuable achievement both for themselves and for their prospective students. Although it was proposed only to CEIT curriculum, this course is designed for prospective students of all departments. For this reason, it is believed that the development of this course is a timely and meaningful contribution to the higher education curriculum in the Faculty of Education.

5.2.1.2. Addressing Different Areas of Interest

The researcher gave different examples from different areas of interest. For example, the cybersecurity issues were explained with non-computer examples. It was found to be favorable for non-CEIT students. It was a natural result of the multidisciplinary nature of the course; the contents of the course were not limited to a specific major.

It is recognized that learners have different majors. For this reason, it is recommended that while explaining the topics, examples should be selected relating to prior knowledge of students from different departments. By doing so, the attention of students towards the lectures could be enhanced. Hence, the interest and participation of the students increase, and they could attain a better grasp of the subject.

5.2.2. Challenging Factors and How They Are Handled

It is found that students' unwillingness to participate in class and online activities and their weak reading habits were challenging factors encountered by the instructor. From the learners' perspective, on the other hand, their inadequacy of English reading and speaking skills, weakness of computer literacy, and difficulty in memorizing the terminology were the leading challenging issues.

The weak reading habit was solved by preparing extended reading notes. Students' participation motivation was depending on grading concerns. Because they were quite sensitive to expected grades, however, an internal motivation to participate in course activities could be developed. In line with this purpose, game-based learning strategies might be employed (Liu & Chu, 2010). Chapman and Rich (2018) conclude in their study that students' motivation is significantly higher in gamified courses.

The information security terms were new topics for non-CEIT students. They underlined that they were concerned about memorizing the terminology, specifically the names of malware types. In both implementations, the researcher provided a word game, and that has motivated the students. However, it was not sufficient to memorize the information. For this reason, a hands on activity and a term project could be assigned to the students. So that they both would use the terms in real life experience and the information is internalized.

The students feel anxious while participating in class activities. The reason they say was their perceived weakness of English-speaking skills. It is a general problem and is not limited to this course (Doiz, Lasagabaster, & Sierra, 2011). In the course, during both the lecture and discussion sessions, the researcher encouraged the students to participate in the course. Besides, during the lectures, explanation of terms in the native language was provided.

5.3. Contributions of the Course to the Learners

The third research question of the study is the perceived contributions of the course. The responses to the interviews and the observational field notes indicate that the course contributed to the students in different ways.

There were several topics which the students reported they have seen in this course for the first time. They stated that they had a chance to learn the topics in detail. The contents of the course reflected the pre-service teachers' teaching related plans. Almost all students concur that what they have learned in this course would be useful in their future careers.

The most immediate influence on the students was the change in their SNS related habits. Almost all students emphasized that they have changed their SNS related behaviors. The use of SNS has been on the rise in the last decades (Jordan & Weller, 2018). There is a high rate of utilization of SNSs among undergraduate students. However, there are various Information security threats on SNSs (Mazzoni & Iannone, 2014; Miller, Parsons, & Lifer, 2010; Ozmen & Atici, 2014). Wisniewski and his company (2012) reported that there are different threats in the use of SNSs. Informing the users about security issues is an important protection measure (Laura, 2015; Wisniewski; Yavanoğlu et al., 2012).

The students emphasized their changed behaviors and raised awareness both in the interviews and during the lecture sessions. The students' in-class discussion participations have also demonstrated this change. For example, in the sixth session of the first implementation, the security of mobile devices was the main topic. The instructor explained the application security and the permissions which the applications asked during the installation. On the discussion session, the second hour of the lecture, the instructor realized that most of the students checked his or her applications and which permissions they have given during the installation.

The students gained the ability to think, talk, and write about cybersecurity. They expressed that they felt more literate and confident while using ICTs. Most of the students stated that they intend to inform their friends and families in case of a privacy breach. The contributions are not limited to the rise in privacy concern, but also the students' ethical sensitivity is also increased. They highlight the limitations of fair use and copyright issues were necessary for their future teaching activities. Furthermore, the interviewees stated that they could use what they have learned during their teaching activities in the future. Particularly, integrating the topics into their instructional materials was the most cited plan for the teaching career.

5.4. Implications and Recommendations

Several suggestions, implications, and recommendations emerged from this study. They are given below.

5.4.1. Implications and Recommendations for Practitioners

The participation in the online activities of the course was not at the expected level. It was mentioned both in the in-class feedback of the students and the responses of the interviewees. The students followed the campus-wide course management system provided by the university. Since the online environment of this course was not located in the university's course management system, some of the students stated that they forgot logging in CEIT215 web site. While designing a course, it is necessary to consider the students' routines. Although there was a link to the course's web site from the campus-wide course management system, the students declared separate web site as a reason for not logging to the course web site.

The potential students of the course were pre-service teachers, and the subtopics were selected accordingly. The contents may be rearranged for students from different faculties, such as engineering or architecture students. Furthermore, the course may be rearranged for adult learning. Before adopting the course for another age, major, or occupation group, a user-related needs analysis is necessary. In this respect, the most frequent security incidents might be explored. Furthermore, a survey could be applied to the students, so that which parts of and to what extent the students know C3 framework topics.

As it was stated in the course objectives, the students are expected to think on C3 issues and be able to discuss related issues. Interaction between the students has important value on critical thinking. For this reason, synchronous and asynchronous discussion methods, such as in-class debates or forum discussions are important methods of instruction.

To increase the students' motivation, one might employ in-class activities or game-based instruction methods. Deficiency of knowledge about the terminology

inhibited the non-CEIT students from participating in in-class discussions. A glossary of terms might be provided at the beginning of the semester.

5.4.2. Implications and Recommendations for the Administrators

This course is proposed as an elective course. In the second implementation, the number of registered students were lower than expected. The main reason was that the schedule conflict of the course in the faculty of education. As a result, since this course is an elective course, it is necessary to schedule the course according to the schedules of other must courses of the potential students.

During the preparatory school and in the first year of the students, the courses aiming at raising reading comprehension skills may be reviewed. In this way, the reading activities in the course might be more efficient.

During the implementation period, the researcher observed informative web pages of universities aiming at providing a guideline for their students. These guidelines included general information on academic integrity, protection of digital identity, and cyberbullying issues. Furthermore, the resources of addiction and cyberbullying were the web sites of NGO and NPO sites. In the universities, to inform and guide the students in different ways, these informative web sites could be launched. Some of the topics include general cybersecurity issues, definition of and encouraging academic integrity and preventing from or dealing with addiction.

5.4.3. Implications and Recommendations for the Policy Makers

ICT and Digital Literacy resources and courses might be included for K12 students. The training attempts might be extended to the parents as well. Citizenship education in Turkey includes general issues about citizenship values, legal rights, and responsibilities. Legal rights and responsibilities regarding digital citizenship might be included in citizenship education.

5.5. Implications and Recommendations for Research

The driving motivation of this study was to explore the critical issues in design, development, and implementation of a course aiming at raising pre-service teachers'

information security awareness and cyberethics sensitivity. Throughout the study, the researcher took several decisions for determining the contents, designing the course outline, and the content sequence. During the implementations, the topics to be taught, weekly course outline, lecture design, and method of the instruction pointed out to consider. At the end of the study, the results indicated that there was a need for such a course, and this course influences pre-service teachers. On the other hand, further studies would be needed.

This course was designed with the guidance of two iterative implementations. Different methods of instruction may be employed to advance learning. Furthermore, for each subject, different teaching methods can be examined. Information security is an evolving topic. The use of ICT diverges into different areas of interest. Cyberethics and security issues on different technologies, such as wearable technologies or the internet of things should be added to the course outline.

This study was conducted in a faculty of education at a state university. The study can be expanded to the other faculties of education of other universities. During the study, the course was designed for pre-service teachers from different majors. Different versions of the course can be developed according to different majors.

During the design and development of the course, pre-service teachers' common information security and cyberethics issues were the focus of interest. The study can be expanded to the administrators and the instructors of teacher training institutions. Furthermore, the contents can be broadened to different disciplines, such as engineering, social sciences, and architecture. This course was designed for users with elementary computer skills as teachers. Individual studies can be employed in raising information security awareness. The studies generally focus on students and teachers. There is a need for an exploration of the misconceptions and prejudgments of administrators regarding their information security and cyberethics beliefs.

At the moment, the design of the course could be considered as having attained a certain level of maturity. However, the continuous development of the course should continue. In the future, further studies can be carried out for formative evaluation.

REFERENCES

Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods. *Behaviour & Information Technology, 33*(3), 236-247. Retrieved from doi: 10.1080/0144929x.2012.708787

Akgun, O. E., & Topal, M. (2015). Eğitim Fakültesi Son Sınıf Öğrencilerinin Bilişim Güvenliği Farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi Örneği. *Sakarya University Journal of Education; 5(20), 98-121.* Retrieved from http://suje.sakarya.edu.tr/article/view/5000109988

Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management, 15*(1), 1650007

Al Awawdeh, S., & Tubaishat, A. (2014, April). An Information Security Awareness Program to Address Common Security Concerns in IT Unit. In *2014 11th International Conference on Information Technology: New Generations* (pp. 273-278). IEEE.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security, 42*, 56-65. doi: 10.1016/j.cose.2014.01.005

Andersson, D., & Reimers, K. (2012). Post-Secondary Education Network Security: Addressing the End User Challenge. In *Edulearn12: 4th International Conference on Education and New Learning Technologies* (pp. 4831-4840). IATED

Andersson, D., Reimers, K., & Barreto, C. (2014). Post-Secondary Education Network Security: Results of Addressing the End User Challenge. In I*NTED2014: 8th International Technology, Education and Development Conference* (pp. 6018-6027).

Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*: Syngress.

Aposto, A. (2016). Choosing the best ID model for your project. Retrieved from http://aaposto.weebly.com/blog/choosing-the-best-id-model-for-your-project

APWG. (2006). Phishing Activity Trends Report *July 2006* Anti-Phishing Working Group.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312. doi: 10.1016/j.chb.2014.05.046

Au, M. H., & Choo, K.-K. R. (2017). Chapter 1 – Mobile Security and Privacy. In M. H. Au & K.-K. R. Choo (Eds.), *Mobile Security and Privacy* (pp. 1-4). Boston: Syngress.

Azari, R. (2003). *Current security management & ethical issues of information technology*. Hershey: IRM Press.

Babad, E. (2001). Students' course selection: Differential considerations for first and last course. *Research in Higher Education, 42*(4), 469-492.

Bada, M., & Sasse, A. (2014, July). *Cybersecurity awareness campaigns: Why do they fail to change behavior?* Global Cyber Security Capacity Centre. Retrieved from http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

Bang, Y., Kim, J., & Hwang, I. S. (2008). *CBR (Case-Based Reasoning) Evaluation Modeling for Security Risk Analysis in Information Security System*. Los Alamitos: IEEE Computer Society.

Barquin, R. C. (1992). In pursuit of a 'ten commandments' for computer ethics. *Computer Ethics Institute*.

Baum, R. M. (2011). Sezen, Sames, and Columbia. *Chemical & Engineering News, 89*.

Beranek, L. (2009). Information systems security education for future teacher at secondary and primary schools. *Journal of Technology and Information Education, 1*(2), 89.

Bereiter, C. (2002). Design Research on Learning Environments. Design Research for Sustained Innovation. *Japanese Cognitive Science Society, 9*(3), 321-327.

Berg, B. L., -. (2009). *Qualitative research methods for the social sciences / Bruce L. Berg* (7th ed).

Berry, J., Vin, H. M., & Ieee. (1996). *Imagery and information over the Defense Red Switch Network.* Paper presented at the Milcom 96, Conference Proceedings, Vols 1-3.

Bilton, N. (2010). Burglars Said to Have Picked Houses Based on Facebook Updates [Blog post]. Retrieved from https://bits.blogs.nytimes.com/2010/09/12/burglars-picked-houses-based-on-facebook-updates/

Borges, J., Martins, J., Andrade, J., & dos Santos, H. (2015). Design of a Case-Based Reasoner for Information Security in Military Organizations. *Proceedings of the 14th European Conference on Cyber Warfare and Security (Eccws-2015)*, 26-34.

Botturi, L., Cantoni, L., Lepori, B., & Tardini, S. (2008). Fast Prototyping as a Communication Catalyst for E-Learning Design *Online and Distance*

Learning: Concepts, Methodologies, Tools, and Applications (pp. 1014-1027). Hershey, PA, USA: IGI Global.

Boulet, G. (2009). Rapid prototyping: An efficient way to collaboratively design and develop e-learning content. *Navy e-learning center of Excellence*.

Bourgeois, D. (2014). The Ethical and Legal Implications of Information Systems In D. T. Bourgeois (Ed.), *Information Systems for Business and Beyond* The Saylor Foundation.

Bradley, T., & Carvey, H. (2006). *Essential computer security: everyone's guide to email, internet, and wireless security*: Elsevier.

Braxton, G. M. (2014). *A study of employee perceived importance, moral sensitivity, judgment and information security policy compliance* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (UMI No: 3609126)

Brouwer, N., & Korthagen, F. (2005). Can Teacher Education Make a Difference? *American Educational Research Journal, 42*(1), 153-224.

Brown, A. L. (1992). Design Experiments: Theoretical and Methodological Challenges in Creating Complex Interventions in Classroom Settings. *Journal of the Learning Sciences, 2*(2), 141-178. doi: 10.1207/s15327809jls0202_2

Buhalis, D. (1998). Strategic Use of Information Technologies in the Tourism Industry. *Tourism Management, 19*(5), 409-421.

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2015, January). Assessing the Role of Security Education, Training, and Awareness on Insiders' Security-related Behavior: An Expectancy Theory Approach. In *2015 48th Hawaii International Conference on System Sciences* (pp. 3930-3940). IEEE

Burridge, G. (2010). Raising a digital child: a digital citizenship handbook for parents. *Learning Media and Technology, 35*(3), 363-364. doi: 10.1080/17439884.2010.481557

Bynum, T. W., & Rogerson, S. (2004). *Computer ethics and professional responsibility*. Malden, MA Blackwell Pub.

Çakır, H., Hava, K., Gülen, Ş. B., & Özüdoğru, G. (2015). Öğretmen adaylarının sosyal ağ sitelerinde güvenlik farkındalıklarının incelenmesi. *Journal of Human Sciences, 12*(1), 16. doi: 10.14687/ijhs.v12i1.3142

Camm, B. (2012). Instructional Design and Rapid Prototyping *eLearning Learning* (Vol. 2018). Minnesota: Dashe&Thompson.

CEIT. (2018). CEIT Course Curriculum, 2019, from http://ceit.metu.edu.tr/en/undergraduate-courses

Çevik, Y. D., & Çoban, T. (2016). Testing Effect in Learning Digital Property and Cyberethics. *SDU International Journal of Educational Studies, 3*(1), 84-99.

Chapman, J. R., & Rich, P. J. (2018). Does educational gamification improve students' motivation? If so, which game elements work best? *Journal of Education for Business, 93*(7), 315-322.

Charest, K. M. (2013). *Factors affecting user behavior and conformance to information security practices: Are end users really the problem?* (Doctoral Dissertation), Retrieved from ProQuest Dissertations & Theses Global database. (Umi No: 3600757)

Chen, I. L., & Shen, L. (2016). The Cyberethics, Cybersafety, and Cybersecurity at Schools. *International Journal of Cyber Ethics in Education (IJCEE), 4*(1), 1-15.

Cherry, D. (2014). *The basics of digital privacy: Simple tools to protect your personal information and your identity online.* Syngress

Christensen, B. M. (2017). Four Quick Ways to Spot Hoax News Stories. [Blog Post] Retrieved from https://www.hoax-slayer.net/four-quick-ways-to-spot-fake-news-stories/

Çiftçi, N. P., & Delialioğlu, Ö. (2016). Supporting students' knowledge and skills in information technology security through a security portal. *Information Development, 32*(5), 1417-1427.

CIS, C. f. I. S. (2017). Know the Rules of Cyber Ethics, from https://www.cisecurity.org/daily-tip/know-the-rules-of-cyber-ethics/

clickbait. 2017. In *Merriam-Webster.com* Retrieved October 12, 2017, from https://www.merriam-webster.com/dictionary/clickbait

Clifford, M. (2012). 15 Strategies Educators Can Use to Stop Cyberbullying. Retrieved from https://www.opencolleges.edu.au/informed/features/15-strategies-educators-can-use-to-stop-cyberbullying/

Yükseköğretim Kurumları Öğrenci Disiplin Yönetmeliği, 7.5.16532 C.F.R. (2012).

CoHE, C. o. H. E. (2018a). *Bilgisayar ve Öğretim Teknolojileri Öğretmenliği Lisans Programı*. Retrieved from http://www.yok.gov.tr/documents/10279/41805112/Bilgisayar_ve_Ogretim_Teknolojileri_Ogretmenligi_Lisans_Programi.pdf.

CoHE, C. o. H. E. (2018b). *Öğretmen Yetiştirme Lisans Programları*. Retrieved from http://www.yok.gov.tr/documents/10279/41805112/AA_Sunus_+Onsoz_Uygulama_Yonergesi.pdf.

Cohen, E., & Cornwell, L. (1989). A question of ethics: Developing information system ethics. *Journal of Business Ethics, 8*(6), 431-437.

Collective, D. (2003). Design-based research: An emerging paradigm for educational inquiry. *Educational Researcher*, 5-8.

Collins, A. (1990). Toward a Design Science of Education. Technical Report No. 1 (pp. 9): Center for Technology in Education New York NY.

Collins, A., Joseph, D., & Bielaczyc, K. (2004). Design Research: Theoretical and Methodological Issues. *Journal of the Learning Sciences, 13*(1), 15-42. doi: 10.1207/s15327809jls1301_2

Conn, K. (2002). *The internet and the law: What educators need to know*: ASCD.

ConnectSafely.org. (2016). 2-Minute Tips: Smart Passwords, from https://www.youtube.com/watch?v=e0ENHKyqRNY

Cooney, M. (2012). Ten common mobile security problems to attack. *PCWorld*, from https://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html

Cox, D. S., Ellis, E. R., Kissel, R., & Kent, K. (2012). *Information security terms: glossary with acronyms and abbreviations*.

Çubukcu, A., & Bayzan, Ş. (2013). Türkiye'de dijital vatandaşlık algısı ve bu algıyı internetin bilinçli, güvenli ve etkin kullanımı ile artırma yöntemleri. *Middle Eastern & African Journal of Educational Research, 5*, 148-174.

Curran, J. M., & Rosen, D. E. (2006). Student Attitudes Toward College Courses: An Examination of Influences and Intentions. *Journal of Marketing Education, 28*(2), 135-148. doi: 10.1177/0273475306288401

Curran, K., Middleton, G., & Doherty, C. (2011). Cheating in exams with technology. *International Journal of Cyber Ethics in Education (IJCEE), 1*(2), 54-62.

Daugherty, J., Teng, Y.-T., & Cornachione, E. (2007). Rapid Prototyping Instructional Design: Revisiting the ISD Model (pp. 8).

Decker, L. G. (2008). *Factors affecting the security awareness of end-users: A survey analysis within institutions of higher learnin* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (UMI NO: 3290951)

Delaney, D., Kummer, T.-F., & Singh, K. (2019). Evaluating the impact of online discussion boards on student engagement with group work. *British Journal of Educational Technology, 50*(2), 902-920. doi: doi:10.1111/bjet.12614

Delialioglu, O. (2011). Bilişim sistemleri güvenliği ve ilgili etik kavramlar. In A. Şentürk (Ed.), *Temel bilgi teknolojileri ve bilgisayar kullanımı* Bursa: Ekin Basım Yayın Dağıtım.

Desforges, C. (2000). *Familiar challenges and new approaches: necessary advances in theory and methods in research on teaching and learning*. Paper presented at the British Educational Research Association Annual Conference, Cardiff. http://www.leeds.ac.uk/educol/documents/00001535.htm

Dikmen, C. H. (n.d.). Siber Zorbalık ve Önleme Yolları Retrieved 2017, November 17, from http://egitimheryerde.net/siber-zorbalik-ve-onleme-yollari/

Doiz, A., Lasagabaster, D., & Sierra, J. M. (2011). Internationalization, multilingualism and English-medium instruction. *World Englishes, 30*(3), 345-359.

Easterday, M., Rees Lewis, D., & Gerber, E. (2014). *Design-based research process: Problems, phases, and applications.* Paper presented at the Proc. of International Conference of Learning Sciences.

Easttom, C. (2016). *Computer security fundamentals*: Pearson IT Certification.

Eaton, S. E. (2013, March 13, 2018). Profile of a cyberbully: 7 Personality traits to watch for. Retrieved from https://drsaraheaton.wordpress.com/2013/04/03/profile-of-a-cyber-bully/

Eaton, S. E. (2017). Cyberbullying among children and teens: A pervasive global issue.

Elekwachi, O. (2002). *End User Computer Security Responsibilities... Know the rules of the game*. SANS Institute 2000 – 2002.

Englander, E. K. (2013). *Bullying and cyberbullying: what every educator needs to know / Elizabeth Kandel Englander*. Cambridge: Cambridge, MA: Harvard Education Press, 2013.

ENISA. (2010). *A new users' guide: How to raise information security awareness.*: The European Network and Information Security Agency (ENISA)

ETCB. (2012). Definition: What does Cyberbullying Exactly Mean? Retrieved November 15, 2017, from http://www.endcyberbullying.org/definition-what-does-cyberbullying-exactly-mean

ETCB. (2013). Five Different Types of Cyberbullying Retrieved November 15, 2017, from http://www.endcyberbullying.org/5-different-types-of-cyberbullying/

ethics. 2018. In Learner's definition of ETHIC, Retrieved October 12, 2017, from http://www.learnersdictionary.com/definition/ethic

Facebook. (2018a). What can I do if I've been phished on Facebook? from www.facebook.com/help/166863010078512

Facebook. (2018b). What is two-factor authentication and how does it work?, from https://www.facebook.com/help/148233965247823

Fairweather, N. B. (2004). Commentary on the "Ten Commandments for Computer Ethics." *Retrieved May 26*, 2009.

Farooq, A., Kakakhel, S. R. U., & Ieee. (2013). *Information Security Awareness: Comparing Perceptions and Training Preferences*. New York: Ieee.

Flores, A. (2014). Think Before You Click (Safety First): YouTube.

Gahran, A. (2012). Most finders of lost phones try to access personal data; survey finds, *CNN Business*. Retrieved from https://edition.cnn.com/2012/03/20/tech/mobile/lost-smartphones-security/index.html

Gallant, D. T. (2011). Protecting Personal Information on Social Networking Sites.. *School Business Affairs, 77*(1), 13-14.

Fikir ve Sanat Eserleri Kanunu, 7981 C.F.R. (1951).

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 5651 C.F.R. (2007).

Gedik, N. (2010). *A design-based research on the use of a blended learning environment* Dissertation

Georgia, S., & Iliada, S. (2014). CyberEthics Case Study *Handbook of Research on Consumerism in Business and Marketing: Concepts and Practices* (pp. 78-90). Hershey, PA, USA: IGI Global.

Gokmen, O. F., & Akgun, O. E. (2015). An Analysis of Computer Education and Instructional Technology Student Teachers' Knowledge of Information Security according to Several Variables. *Çukurova University Faculty of Education Journal, 44*(1), 61-83.

Goodhue, D. L., & Straub, D. W. (1991). Security Concerns of System Users – A Study of Perceptions of the Adequacy of Security. *Information & Management, 20*(1), 13-27. doi: 10.1016/0378-7206(91)90024-v

Greene, T. C. (2004). *Computer security*. Berkeley, CA: Apress.

Grodzinsky, F. S., & Wolf, M. J. (2009). Ethical Interest in Free and Open Source Software *The Handbook of Information and Computer Ethics* (pp. 245-271): John Wiley & Sons, Inc.

Gupta, M., & Sharman, R. (2008). *Social and Human Elements of Information Security: Emerging Trends and Countermeasures: Emerging Trends and Countermeasures*: IGI Global.

Gustafson, K. L., & Branch, R. M. (1997). Revisioning models of instructional development. *Educational Technology Research and Development, 45*(3), 73-89.

Hamiti, M., Reka, B., & Baloghová, A. (2014). Ethical Use of Information Technology in High Education. *Procedia – Social and Behavioral Sciences, 116*, 4411-4415. doi: http://dx.doi.org/10.1016/j.sbspro.2014.01.957

Hanus, B. T. (2014). *The impact of information security awareness on compliance with information security policies: A phishing perspective* (Doctoral dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (UMI NO: 3727160)

Heick, T. (2013). The Definition Of Digital Citizenship. Retrieved from https://www.teachthought.com/the-future-of-learning/the-definition-of-digital-citzenship/

Hemamali, T. (2015). Information Security and Privacy in Social Media: The Threat Landscape *Implications of Social Media Use in Personal and Professional Settings* (pp. 73-101). Hershey, PA, USA: IGI Global.

Henderson, M., Auld, G., & Johnson, N. F. (2014). *Ethics of teaching with social media.* Paper presented at the Australian Computers in Education Conference, Adelaide, SA.

Herrington, J., McKenney, S., Reeves, T., & Oliver, R. (2007). Design-based research and doctoral students: Guidelines for preparing a dissertation proposal.

Hess, J.L., & Whittington, M.S. (2003). Developing an effective course syllabus. *North Amer. College Teachers Agr. J., 47*(3), 23-27.

HHS. (2015a). How to Prevent Bullying, Retrieved November 15, 2017, from http://www.stopcyberbullying.org/prevention/index.html

HHS. (2015b). What is Bullying. Retrieved November 15, 2017, from https://www.stopbullying.gov/cyberbullying/what-is-it/

Higgin, T. (2017). Protecting Student Privacy on Social Media. Retrieved from https://www.edutopia.org/article/protecting-student-privacy-social-media

How, L. (2017). 5 Steps to Recognize Fake Facebook Accounts: YouTube.

Infographics, T. (2015). The Do's and Don'ts for Teachers on Social Media Infographic. Retrieved from https://elearninginfographics.com/dos-donts-teachers-social-media-infographic/

Irene, L. C., & Libi, S. (2016). The Cyberethics, Cybersafety, and Cybersecurity at Schools. *International Journal of Cyber Ethics in Education (IJCEE), 1*(4), 1-15. doi: 10.4018/ijcee.2016010101

ISO. (2009). Information technology – Security techniques – Information security management systems – Overview and vocabulary. ISO/IEC, 2018, from https://www.iso.org/obp/ui#iso:std:iso:tr:11633:-2:ed-1:v1:en:term:2.9

ISO. (2017). ISO/IEC 27000 family – Information security management systems, 2018, from https://www.iso.org/isoiec-27001-information-security.html

ISO. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary *ISO/IEC 27000* (Vol. 2018-02).

ITS, I. T. S. (2017). Physical Security, from https://its.ucsc.edu/security/physical.html

ITU. (2008). *Series X: Data Networks, Open System Communications and Security Telecommunication security*. International Telecommunication Union (ITU).

ITU. (2015). Global Cybersecurity Index & Cyberwellness Profiles (I. C. Team, Trans.). In M. Minges (Ed.), (pp. 528): International Telecommunication Union (ITU).

Ivester, M. (2011). *Lol-- omg! : what every student needs to know about online reputation management, digital citizenship, and cyberbullying / Matt Ivester*. Reno, NV: Serra Knight Pub.

Jacobson, D., & Idziorek, J. (2016). *Computer security literacy: Staying Safe in a Digital World*. Boca Raton: CRC Press / Taylor & Francis Group.

Johnson, D. (2007). Teaching Students Right from Wrong in the Digital Age. Retrieved from http://twaterman.pbworks.com/f/ethics_doug_johnson.pdf

Jones, T., & Richey, R. (2000). Rapid prototyping methodology in action: A developmental study. *Educational Technology Research and Development, 48*(2), 63-80-80. doi: 10.1007/bf02313401

Jordan, K., & Weller, M. (2018). Academics and Social Networking Sites: Benefits, Problems and Tensions in Professional Engagement with Online Networking. *Journal of Interactive Media in Education, 2018*(1).

Karjalainen, M., & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems, 12*(8), 518-555.

Karlsson, F., & Hedström, K. (2014). *End User Development and Information Security Culture.* Paper presented at the Human Aspects of Information Security, Privacy, and Trust, Cham.

Katz, F. H. (2005). *The effect of a university information security survey on instruction methods in information security*. Paper presented at the Proceedings of the 2nd annual conference on Information security curriculum development, Kennesaw, Georgia.

Keengwe, J., & Agamba, J. (2012). Pre-Service Teachers' Perceptions of Information Assurance and Cybersecurity. *Int. J. Inf. Commun. Technol. Educ., 8*(2), 94-101. doi: 10.4018/jicte.2012040108

Kelly, A. (2013). When is design research appropriate *Educational design research* (pp. 135-150).

Kimmons, R., & Veletsianos, G. Teacher Professionalization in the Age of Social Networking Sites. *Learning, Media and Technology, 40*(4), 480-501.

Klein, B., Moss, G., & Edwards, L. (2015). *Understanding copyright: intellectual property in the digital age*: Los Angeles, California: SAGE, 2015.

Korovessis, P. (2011). Information Security Awareness in Academia. *International Journal of Knowledge Society Research (IJKSR), 2*(4), 1-17. doi: 10.4018/jksr.2011100101

Shariff, S., & Churchill, A. H. (2010). *Truths and myths of cyber-bullying: International perspectives on stakeholder responsibility and children's safety* (Vol. 38): Peter Lang.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security, 27*(5–6), 224-231. doi: http://dx.doi.org/10.1016/j.cose.2008.05.006

Kritzinger, E., & von Solms, S. H. (2010). Cybersecurity for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847. doi: 10.1016/j.cose.2010.08.001

Kruger, R. (2003). Discussing cyberethics with students is critical. *The Social Studies, 94*(4), 188-189.

Kruse, K. (2004). Introduction to instructional design and the ADDIE model. *Transformative Designs*, 2018, Retrieved from http://transformativedesigns .com/id_systems.html

Kuehn, L. (2012). ManageYourDigital Footprint. *Our Schools Our Selves, 21*(2), 3.

Kuss, D. J., & Griffiths, M. D. (2017). Social networking sites and addiction: Ten lessons learned. *International journal of environmental research and public health, 14*(3), 311.

Lachman, V. D. (2013). Social media: managing the ethical issues. *Medsurg Nursing, 22*(5), 326-330.

Laura, A.-F. (2015). Social Media in Higher Education: Examining Privacy Concerns among Faculty and Students *Implications of Social Media Use in Personal and Professional Settings* (pp. 1-24). Hershey, PA, USA: IGI Global.

Lehto, M. (2015). *Cybersecurity Competencies – Cyber Security Education and Research in Finnish Universities*. Paper presented at the Proceedings of the 14th European Conference on Cyber Warfare and Security (Eccws-2015), Hatfield. https://jyx.jyu.fi/handle/123456789/46540

Leshin, C. B., Pollock, J., & Reigeluth, C. M. (1992). *Instructional design strategies and tactics*: Educational Technology.

Liu, T.-Y., & Chu, Y.-L. (2010). Using ubiquitous games in an English listening and speaking course: Impact on learning outcomes and motivation. *Computers & Education, 55*(2), 630-643. Retrieved from doi: 10.1016/ j.compedu.2010.02.023

Ma, H. J., Wan, G., & Lu, E. Y. (2008). Digital cheating and plagiarism in schools. *Theory Into Practice, 47*(3), 197-203.

Mathiesen, K. (2009). Censorship and Access to Expression *The Handbook of Information and Computer Ethics* (pp. 571-587): John Wiley & Sons, Inc.

Mazzoni, E., & Iannone, M. (2014). From High School to University: Impact of Social Networking Sites on Social Capital in the Transitions of Emerging Adults. *British Journal of Educational Technology, 45*(2), 303-315.

McKenney, S. (2001). *Computer-based support for science education materials developers in Africa: Exploring potentials.* Doctoral Dissertation, UT, Enschede. Retrieved from https://ris.utwente.nl/ws/portalfiles/portal/6080267/ thesis_S_McKenney.pdf (9789036516426)

Merkow, M. S., & Breithaupt, J. (2014). *Information security: Principles and practices*: Pearson Education.

Mert, M., Bülbül, H. İ., & Sağıroğlu, Ş. (2012). Milli Eğitim Bakanlığına Bağlı Okullarda Güvenli İnternet Kullanımı. *TÜBAV Bilim Dergisi, 5*(2), 12.

METU-CC. (2014). What is phishing? Retrieved September 23, 2017 from METU Computer Center Website: https://faq.cc.metu.edu.tr/faq/what-phishing

METU. (2008). METU Information Technology Resources Use Policy from http://www.metu.edu.tr/it-use-policy

METU. (2017). Code of Ethics & Core Values. Retrieved October, 5th, 2018

Miller, R., Parsons, K., & Lifer, D. (2010). Students and Social Networking Sites: The Posting Paradox. *Behaviour & Information Technology, 29*(4), 377-382.

Misenheimer, K. J. (2014). *Exploring Information Technology Security Requirements for Academic Institutions to Reduce Information Security Attacks, Breaches, and Threats* (Doctoral Dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (UMI No: 3638473)

MoNE, M. E. B.-M. (2012). *Milli Eğitim Bakanlığı Bilgi ve Sistem Güvenliği Yönergesi*. Ankara.

MoNE, M. E. B.-M. (2016). *Bilgi Güvenliği*, Ankara. Retrieved from MoNE Website: http://bidb.meb.gov.tr/www/bilgi-guvenligi/dosya/8

MoNE, M. E. B.-M. (2017a). *Milli Eğitim Bakanlığı Bilgi ve Sistem Güvenliği Yönergesi*. Ankara.

Okullarda Sosyal Medyanın Kullanılması Hakkında Genelge (2017b).

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security, 59*, 186-209. doi: 10.1016/j.cose.2016.03.004

MSFTOnlineSafety. (2014). Oversharing?: Retrieved from YouTube website: https://www.youtube.com/watch?v=D1NQPUk1CHo

Mutchler, L. A. (2012). *Expanding protection motivation theory: The role of individual experience in information security policy compliance* (Doctoral Dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (UMI No: 3546556)

Nalwa, K., & Anand, A. P. (2003). Internet Addiction in Students: A Cause of Concern. *CyberPsychology & Behavior, 6*(6), 653-656. doi: 10.1089/109493103322725441

NIST. (2013). Glossary of Key Information Security Terms In R. Kissel (Ed.): National Institute of Standards and Technology Computer Division.

Oh, E., & Reeves, T. C. (2010). The implications of the differences between design research and instructional systems design for educational technology researchers and practitioners. *Educational Media International, 47*(4), 263-275. doi: 10.1080/09523987.2010.535326

ÖİDB. (2011). Academic Integrity Guide for Students. Retrieved October 5, 2018, from OIDB Web site: http://oidb.metu.edu.tr/en/system/files/Academic Integrity Guide for Students.pdf

OpenDNS. (2017). PHISHING QUIZ – Think you can Outsmart Internet Scammers? 2018, Retrieved from https://www.opendns.com/phishing-quiz/

Owusu-Acheaw, M., & Larson, A. G. (2014). Reading habits among students and its effect on academic performance: A study of students of Koforidua Polytechnic. *Library philosophy and practice*, 0_1.

Özer, E. A., & Özer, Ü. (2018). *Sınıf Öğretmeni Adaylarının Dijital Vatandaşlık Eğitimi İhtiyaçları.* Paper presented at the ICPESS (International Congress on Politic, Economic and Social Studies).

Ozmen, B., & Atici, B. (2014). Learners' Views Regarding the Use of Social Networking Sites in Distance Learning. *International Review of Research in Open and Distance Learning, 15*(4), 21-42.

Perez, M., Berry, R., & Hollman, C. (2003). Information Technology Security Awareness in Academia: An Initial Assessment. *Issues in Information Systems, 4*, 660-666.

Phishing.org. (2018). What Is Phishing?

Pinterest. (2018). Two-factor authentication. Retrieved from https://help.pinterest.com /en/article/two-factor-authentication.

Pipkin, D. L. (2000). *Information security: protecting the global enterprise*: Prentice-Hall, Inc.

Plotkin, R. (2012). *Computer ethics*. New York, NY: Facts On File.

Poll, H. (2015). Pearson Student Mobile Device Survey: Grades 4 through 12.

Prensky, M. (2001). Digital natives, digital immigrants part 1. *On the horizon, 9*(5), 1-6.

Pruitt-Mentle, D. (2000). *C3 Framework Cyberethics, Cybersafety and Cybersecurity Promoting Responsible Use*. Paper presented at the Educational Technology Policy, Research and Outreach. http://www.edtechpolicy.org/cyberk12/ Documents/C3Awareness/C3_framework_full_final.pdf

Pruitt-Mentle, D., & Pusey, P. (2010). State of K12 cyberethics, safety and security curriculum in US: 2010 Educator opinion. *Educational technology policy, Research and Outreach*.

Pryor, S., Martinez, M., & Pugliese, N. (2012). *Ethical and professional dilemmas for educators*. Retrieved from https://portal.ct.gov/-/media/SDE/TEAM/ Module_5_Facilitator_Guide_January_2015.pdf.

Pusey, P., & Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82-85.

PuzzleMaker. (2017). PuzzleMaker, from http://www.discoveryeducation.com/free-puzzlemaker

Reeves, T. C. (2006). Design research from a technology perspective. *Educational design research, 1*(3), 52-66.

Reigeluth, C. M. (1983). *Instructional-design theories and models*. Hillsdale, N.J.: Lawrence Erlbaum Associates.

Reiser, R. A. (2001). A history of instructional design and technology: Part II: A history of instructional design. *Educational Technology Research and Development, 49*(2), 57-67. doi: 10.1007/bf02504928

Ribble, M. S. (2006). *Implementing digital citizenship in schools: The research, development and validation of a technology leader's guide.* Ed.D. Retrieved from ProQuest Dissertations & Theses Global database. (UMI No: 3223358)

Ribble, M. S. (2009). Digital Citizenship from http://www.digitalcitizenship.net/

Ribble, M. S. (2011). *Digital Citizenship in Schools* (Vol. 2nd ed). Eugene, Or: International Society for Technology in Education (ISTE).

Richey, R. C. (1994). *Developmental Research: The Definition and Scope*. Paper presented at the National Convention of the Association for Educational Communications and Technology, Nashville. Information Analyses Reports – Evaluative Speeches/Meeting Papers retrieved from http://files.eric.ed.gov/fulltext/ED373753.pdf

Riola, P. A. (2014). *Examining smartphone security behavior of college students* (Doctoral Dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (UMI No: 3618138)

Roberts, L. (1983). The Darsee Case. Harvard's Handling of Fraud: Good Intentions Are Not Enough. *BioScience, 33*(6), 358-364.

Roberts, T. S. (2008). Student Plagiarism in an Online World: An Introduction *Student Plagiarism in an Online World: Problems and Solutions* (pp. 1-9). Hershey, PA, USA: IGI Global.

Robinson, L. (2010). *Security vs. access: balancing safety and productivity in the digital school / LeAnne K. Robinson, Abbie H. Brown, Tim D. Green*.

Rouse, M. (2012, December 2015). *Cyberbullying*. Retrieved October 5, 2017, from https://whatis.techtarget.com/definition/cyberbullying

Rouse, M. (2013). Creative Commons. Retrieved October 5, 2018, from https://whatis.techtarget.com/definition/Creative-Commons-copyright

Ryan, J. E. (2006). *A comparison of information security trends between formal and informal environments* (Doctoral Dissertation) Retrieved from ProQuest Dissertations & Theses Global database. (UMI No: 3225287)

San Nicolas-Rocca, T., & Olfman, L. (2013). End User Security Training for Identification and Access Management. *Journal of Organizational and End User Computing, 25*(4), 75-103. doi: 10.4018/joeuc.2013100104

Sevim, N., İslim, Ö. F., & Kaplan Akilli, G. (2016). Bilişim Teknolojileri Öğretmen Adaylarının Bölümlerine Yönelik Algısı: ODTÜ BÖTE Örneği. *Journal of Kirsehir Education Faculty, 17*(1).

Sezer, B., Yilmaz, R., & Karaoglan Yilmaz, F. G. (2015). Cyberbullying and teachers' awareness. *Internet Research, 25*(4), 674-687. doi: 10.1108/IntR-01-2014-0023

Shea, V. (2004). Netiquette S. T. Ross (Ed.) Retrieved from http://www.albion.com/netiquette/

Shenton, A. K. (2004). Strategies for Ensuring Trustworthiness in Qualitative Research Projects. *Education for Information, 22*(2), 63-75.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41. doi: doi:10.1108/09685220010371394

Smith, R. E. (2015). *Elementary information security*: Jones & Bartlett Publishers.

Smith, R. E. (2016). Elementary Information Security (pp. xx, 890 p.). Retrieved from http://proquestcombo.safaribooksonline.com/book/networking/security/9781284055931

Solms, R. v., & Niekerk, J. v. (2013). From information security to cybersecurity. *Computers & Security, 38*, 97-102. doi: https://doi.org/10.1016/j.cose.2013.04.004

Souppaya, M., & Scarfone, K. (2013). Guidelines for managing the security of mobile devices in the enterprise. *NIST Special Publication, 800*, 124.

Spacey, J. (2017). Digital Identity, from https://simplicable.com/new/digital-identity

Spinello, R. A. (2008). Intellectual Property: Legal and Moral Challenges of Online File Sharing. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 553-569). Hoboken, New Jersey: John Wiley & Sons, Inc.

Stahl, B. C. (2009). Ethical Issues of Information and Business *The Handbook of Information and Computer Ethics* (pp. 311-335): John Wiley & Sons, Inc.

Stahl, B. C., Moira, C.-M., & Peter, N. (2006). Forensic Computing: The Problem of Developing a Multidisciplinary University Course *Digital Crime and Forensic Science in Cyberspace* (pp. 291-310). Hershey, PA, USA: IGI Global.

Steinberg, S. (2017a). Child Privacy with Stacy Steinberg: Retrieved from YouTubewebsite: https://www.youtube.com/watch?v=csbojK4XWVw.

Steinberg, S. (2017b). Sharenting Risks: Retrieved from YouTube website: https://www.youtube.com/watch?v=lCdSMNFl69I.

Szuba, T. (1998). Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security (pp. ix, 141 p.). Retrieved from https://nces.ed.gov/pubs98/98297.pdf

Tasevski, P. (2015). IT and Cyber Security Awareness – Raising Campaigns. *Information & Security: An International Journal, 34*. doi: http://dx.doi.org/10.11610/isij.350x

Tavani, H. T. (2013). Cyberethics. In A. L. C. Runehov & L. Oviedo (Eds.), *Encyclopedia of Sciences and Religions* (pp. 565-570). Dordrecht: Springer Netherlands.

Techopedia. (Ed.) (2017) Techopedia.

TechTarget. (2017). Mobile Security, Retrieved from http://whatis.techtarget.com/definition/mobile-security

TechTarget. (2018). Digital Identity, Retrieved from http://whatis.techtarget.com/definition/digital-identity

Thomson, M. E., & Solms, R. v. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security, 6*(4), 167-173. doi: doi:10.1108/09685229810227649

Timm, D. M., & Duven, C. J. (2008). Privacy and Social Networking Sites. *New Directions for Student Services*(124), 89-102.

Tripp, S. D., & Bichelmeyer, B. (1990). Rapid prototyping: An alternative instructional design strategy. *Educational Technology Research and Development, 38*(1), 31-44.

Tse, D. W. K., Tse, W. K. F., Ling, M. L., Lai, S. M., Tevanotai, A., & IEEE. (2014). Awareness in e-Banking Security and Usage. *2014 International Conference on Information Science, Electronics and Electrical Engineering (IEEE)*, Sapporo, 2014, pp. 1176-1150. doi: 10.1109/InfoSEEE.2014.6947856

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective, 17*(5-6), 207-227. doi: 10.1080/19393550802492487

Tuana, N. A., & Vasko, S. E. (2015). Ethical Sensitivity Retrieved from http://stem-researchethics.org/morallit/node/119

Tully, S., & Mohanraj, Y. (2017). Chapter 2 – Mobile Security: A Practitioner's Perspective. In M. H. Au & K.-K. R. Choo (Eds.), *Mobile Security and Privacy* (pp. 5-55). Boston: Syngress.

Üçgül, M. (2012). *Design and development issues for educational robotics training camps* (Doctoral dissertation) Retrieved from METU E-Theses Database

Van den Akker, J. (1999). Principles and Methods of Development Research. In J. Van den Akker, R. M. Branch, K. Gustafson, N. Nieveen & T. Plomp (Eds.), *Design Approaches and Tools in Education and Training* (pp. 1-14). Dordrecht: Springer Netherlands.

Van den Akker, J., Bannan, B., Kelly, A. E., Nieveen, N., & Plomp, T. (2013). Educational design research. In N. N. Tjeerd Plomp (Ed.), *Educational design research*. Enschede: Netherlands Institute for Curriculum Development (SLO).

Van den Akker, J., Gravemeijer, K., McKenney, S., & Nieveen, N. (2006). *Educational design research*: Routledge.

Waddell, S. A. (2013). *A study of the effect of information security policies on information security breaches in higher education institutions* (Doctoral Dissertation). Retrieved from ProQuest Dissertations & Theses Global database. (UMI No: 3604516)

Waly, N., Tassabehji, R., Kamala, M. (2012). Improving Organisational Information Security Management: The Impact of Training and Awareness. *2012 IEEE 14th International Conference on High-Performance Computing and Communications & 2012 IEEE 9th International Conference on Embedded Software and Systems (Hpcc-Icess)*, p 1270-1275. doi: 10.1109/hpcc.2012.187

Wang, F., & Hannafin, M. J. (2005). Design-based research and technology-enhanced learning environments. *Educational Technology Research and Development, 53*(4), 5-23. doi: 10.1007/bf02504682

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston, MA: Course Technology.

Wikibooks, c. (2016, 9 June 2016). Information Security in Education Retrieved October 20, 2018, from https://en.wikibooks.org/wiki/Information_Security_in_Education

WikipediaContributors. (2017). Trolley problem Retrieved November 22, 2017, from https://en.wikipedia.org/w/index.php?title=Trolley_problem&oldid=878238897

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication, 800*, 50.

Wisniewski, P. J. (2012) *Understanding and Designing for Interactional Privacy Needs within Social Networking Sites* (Doctoral Dissertation). Retrieved from: http://www.proquest.com/en-US/products/dissertations/individuals.shtml.

Wood, C. C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security, 2004*(1), 16-17. doi: https://doi.org/10.1016/S1361-3723(04)00019-3

Woodhouse, S. (2007). *Information security: End user behavior and corporate culture*. Los Alamitos: Ieee Computer Soc.

WTS. (2017). Plagiarism: What It is and How to Recognize and Avoid It. Retrieved October 7, 2018, from https://wts.indiana.edu/writing-guides/plagiarism.html

Yakın, İ. (2012). *The Design, development and evaluation of an electronic performance support system (EPSS) for the crime scene investigation unit* Ph.D., ODTÜ, Ankara.

Yavanoğlu, U., Sağıroğlu, Ş., & Çolak, İ. (2012). Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler. *Politeknik Dergisi, 15*(1), 15-27.

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Öğretmenlerin Dijital Veri Güvenliği Farkındalığı. *Sakarya University Journal of Education, 6*(2), 20. doi: 10.19126/suje.29650

Zamora, W. (2016, October, 15). Top 10 ways to secure your mobile phone. [Blog Post] Retrieved from https://blog.malwarebytes.com/101/2016/09/top-10-ways-to-secure-your-mobile-phone/

APPENDICES

A. References to the Review of the Surveys in Needs Analysis Phase

Allam, S., Flowerday, S. V., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. *Computers & Security, 42*, 56-65. doi: 10.1016/j.cose.2014.01.005

Çakır, H., Hava, K., Gülen, Ş. B., & Özüdoğru, G. (2015). An investigation of pre-service teachers' security awareness on social networking sites Öğretmen adaylarının sosyal ağ sitelerinde güvenlik farkındalıklarının incelenmesi. *Journal of Human Sciences, 12*(1), 887-902 doi: 10.14687/ijhs.v12i1.3142

Cole, S., & McCabe, D. L. (1996). Issues in academic integrity. *New Directions for Student Services, 1996*(73), 67-77.

Hanus, B. T. (2014). *The impact of information security awareness on compliance with information security policies: A phishing perspective.* 3727160 Ph.D., University of North Texas, Ann Arbor. Retrieved from http://search.proquest.com/docview/1719103457?accountid=13014 ProQuest Dissertations & Theses Global database.

Kaya, A., & Kaya, B. (2014). Öğretmen adaylarının dijital vatandaşlık algısı. *International Journal of Human Sciences, 11*(2), 346-361. doi: 10.14687/ijhs.v11i2.2917

Kidwell, L. A. (2001). Student Honor Codes as a Tool for Teaching Professional Ethics. *Journal of Business Ethics, 29*(1), 45-49. doi: 10.1023/a:1006442925586

Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health, 41*(6), S22-S30.

Kuss, D. J., & Griffiths, M. D. (2011). Excessive online social networking: Can adolescents become addicted to Facebook? *Education and Health, 29*(4), 63-66.

Kuss, D. J., & Griffiths, M. D. (2017). Social networking sites and addiction: Ten lessons learned. *International journal of environmental research and public health, 14*(3), 311.

Ma, H. J., Wan, G., & Lu, E. Y. (2008). Digital Cheating and Plagiarism in Schools. *Theory Into Practice, 47*(3), 197-203. doi: 10.1080/00405840802153809

Maramark, S., & Maline, M. B. (1993). *Academic Dishonesty Among College Students. Issues in Education.* U.S. Department of Education.

McCabe, D. L., Trevino, L. K., & Butterfield, K. D. (1999). Academic integrity in honor code and non-honor code environments: A qualitative investigation. *The Journal of Higher Education, 70*(2), 211-234.

McNaught, C., & Kennedy, D. M. (2009). Bilingual Plagiarism in the Academic World. In *Ethical Practices and Implications in Distance Learning* (pp. 320-327). Hershey, PA, USA: IGI Global.

Nalwa, K., & Anand, A. P. (2003). Internet Addiction in Students: A Cause of Concern. *CyberPsychology & Behavior, 6*(6), 653-656. doi: 10.1089/109493103322725441

Poll, H. (2015). Pearson Student Mobile Device Survey: Grades 4 through 12. Retrieved 25 November 2018, from: https://www.pearsoned.com/wp-content/uploads/Pearson-K12-Student-Mobile-Device-Survey-050914-PUBLIC-Report.pdf

Riola, P. A. (2014). *Examining smartphone security behavior of college students.* 3618138 Ph.D., Northcentral University, Ann Arbor. Retrieved from http://gradworks.umi.com/36/18/3618138.html http://search.proquest.com/docview/1528556586?accountid=13014 ProQuest Dissertations & Theses Global database.

Sezer, B., Yilmaz, R., & Karaoglan Yilmaz, F. G. (2015). Cyberbullying and teachers' awareness. *Internet Research, 25*(4), 674-687. doi: 10.1108/IntR-01-2014-0023

Thompson, B. C., Mazer, J. P., & Flood Grady, E. (2015). The Changing Nature of Parent–Teacher Communication: Mode Selection in the Smartphone Era. *Communication Education, 64*(2), 187-207. doi: 10.1080/03634523.2015.1014382

TUIK. (2018). Temel İstatistikler. Retrieved 25 November 2018, from http://tuik.gov.tr/UstMenu.do?metod=temelist

Yıldırım, N., & Varol, A. (2013). Sosyal Ağlarda Güvenlik: Bitlis Eren ve Fırat Üniversitelerinde Gerçekleştirilen Bir Alan Çalışması. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 6*(1).

B. Course Proposal Form for CEIT 215 (Pre-implementation Phase)

COURSE PROPOSAL

Catalog Description
The goal of the course is to raise the information security awareness and cyberethics sensitivity of pre-service teachers. This course addresses several of the major security, ethical and policy issues that are changing the way educators think about new information and communication technologies in a classroom setting. While covering information security and cyberethics concepts, the course also demonstrates several real-life cases. The course will cover but not limited to topics such as safety in social media, netiquette, acceptable use of computing resources, electronic cheating, high-tech hate speech, intellectual property, digital divide, social equity, copyright, and current governmental regulations. During the course from time to time, students will have a chance to hear from several information technology experts on above course topics.

Course Objectives and Goals
The goal of the course is to raise the information security awareness and cyberethics sensitivity of pre-service teachers. The course will cover not only information security and cyberethics concepts but also provide several case activities. By the end of the course, students will • have a higher awareness of legal policies regarding cybersecurity and ethics • be able to identify and describe the ethical issues related to the use of computers and technology integration in schools • be able to talk about the responsibilities of parents, teachers as well as the community for establishing new interactions involving any type of ICT based communications • be able to identify and describe responsible behavior on social media • be able to establish new classroom policies and procedures to ensure consistency with fair use guidelines on information security and child protection • be able to raise awareness and share knowledge on important issues regarding cyberbullying • be able to protect personal information as well as hardware assets • be able to backup & restore personal information assets • be able to recognize and describe security threats and phishing attempts.

Course Outline	
Week 1:	Information security and cyberethics
Week 2:	Principle issues on cyberethics and information security for educators. • Code of ethics on the information technology
Week 3:	• Ethical issues on teaching activities, • Responsibilities on students' privacy, • Online interaction issues from an ethical perspective.
Week 4:	Copyright issues, • Intellectual property, • Fair use of digital sources
Week 5:	Plagiarism • Plagiarism detection software • Citation issues
Week 6:	Social Media • What should teachers know about social media? • Threats, security issues and precautions on social media • Privacy issues and sharenting • Detection and prevention from malicious profiles
Week 7:	Cyberbullying
Week 8:	Digital divide
Week 9:	Cyberethics
Week 10:	Security policy and ethics regulations • Case of Middle East Technical University • Case of Ministry of National Education
Week 11:	Hoaxes and viruses
Week 12:	Ethical hacking • White-hat hackers • Social engineering
Week 13:	Identity theft • Phishing • Passwords protecting
Week 14:	Hardware security • Virus protection, • backing up and restoring

Justification of the Course Proposal
The recent developments in information communication technologies (ICT) caused new concerns in education from ethical and security perspective. Recent research studies related to information security generally focus on business and commercial settings. As a result, the major motivation for users' awareness of information security threats focuses on financial or professional concerns. In an educational setting, on the other hand, the nature of ICT infrastructure and the roles of end users are completely different compared to that of business settings. School teachers, students, and non-ICT administrative employees are end users of ICT systems of an educational institution. There are several models for raising end users' information security awareness level, but there is no certain method for pre-service teachers. Pre-service teachers are not only expected to be aware of information security issues but also they must be well trained to transfer the concepts about information security and cyberethics to their prospective students about these issues. Pre-service teachers are also expected to have a sense of ethical concerns from two perspectives: (i) their teaching activities in the future, and (ii) their students' cybersafety issues.

Textbook
• Azari, R. (2003). Current security management & ethical issues of information technology. Hershey: IRM Press. • Plotkin, R. (2012). Computer ethics. New York, NY: Facts on File. • Szuba, T. (1998). Safeguarding your technology: practical guidelines for electronic education information security. (https://nces.ed.gov/pubs98/safetech/)

Reference Books
• Bynum, T. W., & Rogerson, S. (2004). Computer ethics and professional responsibility. Malden, MA Blackwell Pub. • Benson, V., & Morgan, S. (2015). Implications of Social Media Use in Personal and Professional Settings (pp. 1-362). Hershey, PA: IGI Global. doi:10.4018/978-1-4666-7401-1 http://www.igi-global.com/gateway/book/115502) • Information Security in Education. (2016, June 9). Wikibooks, the Free Textbook Project. Retrieved April 19, 2017, from https://en.wikibooks.org/wiki/Information_Security_in_Education • Gupta, M., & Sharman, R. (2009). Handbook of research on social and organizational liabilities in information security. Hershey, PA: Information Science Reference.

C. The Consent Form and Interview Protocol

Bu çalışma ODTÜ Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü doktora öğrencisi Evrim AKMAN KADIOĞLU tarafından Yrd. Doç. Dr. Cengiz Savaş AŞKUN danışmalığında doktora tez çalışması olarak yürütülmektedir. Çalışmanın amacı, öğretmen adayları için bilgi güvenliği farkındalığı ve bilişim etik duyarlılığını arttırmaya yönelik bir ders geliştirmek ve bu dersin tasarım, geliştirme ve uygulama aşamalarını etkileyen faktörleri araştırmaktır. Bu amaca yönelik olarak sizinle yaklaşık 10-20 dakika arası sürecek bir mülakat yapılacaktır ve sizin onay vermeniz durumunda görüşme bir ses kayıt cihazı ile kaydedilecektir. Cevaplarınız gizli tutulacak ve sadece araştırmacılar tarafından değerlendirilecektir; elde edilecek bilgiler doktora tezinde ve bilimsel yayımlarda kullanılacaktır. Çalışmanın hiçbir aşamasında kimlik belirleyici bilgiler kullanılmayacaktır.

Çalışmaya katılım tamamen gönüllülük esasına dayanmaktadır. Görüşme genel olarak kişisel rahatsızlık verecek sorular içermemektedir. Ancak görüşme esnasında sorulardan ya da herhangi başka bir nedenden ötürü kendinizi rahatsız hissederseniz görüşmeyi istediğiniz zaman bırakabilirsiniz.

Bu çalışmaya katıldığınız için şimdiden teşekkür ederiz. Bu çalışmayla ilgili daha fazla bilgi almak isterseniz ODTÜ Bilgisayar ve Öğretim Teknolojileri Eğitimi bölümü doktora öğrencisi Evrim AKMAN KADIOĞLU (eakman@metu.edu.tr) ya da aynı bölüm öğretim üyesi Yrd. Doç. Dr. Cengiz Savaş AŞKUN (askun@metu.edu.tr) ile iletişime geçebilirsiniz.

Çalışmaya katılmayı onaylıyor musunuz?

CEIT 215 Dersi Görüşme Protokolü

1) Bu derste daha evvelden bildiğiniz konular var mıydı? Ön bilginizin kaynağı neydi?
2) İlk kez bu derste gördüğünüz konular nelerdi?
3) Yanlış bildiğinizi farkettiğiniz konular nelerdi?
4) Birebir etkisini gördüğünüz konular var mıydı? Varsa nelerdi? Nasıl bir etki gördünüz?
5) Bu derste edindiğiniz bilgileri öğretmenlik hayatınızda nasıl kullanmayı düşünürsünüz?
6) Sosyal medyayı öğretmenlik sürecinizde kullanmayı düşünüyor musunuz?
7) Bu dersle ilgili iyileştirilmesi gerektiğini gerektiğini düşündüğünüz konular var mı?
8) Dersle ilgili en beğendiğiniz özellik neydi?
9) Dersle ilgili en beğenmediğiniz özellik neydi?
10) Dersle ilgili en zorlandığınız kısım/özellik/konu neydi?
11) Eklemek istediğiniz bir şey var mı?

CEIT 215 Interview Protocol

1. In this course, were there any subject that you already knew about? What was the source of your prior knowledge?
2. What were the subjects you first learned in this course?
3. What were your misconceptions?
4. Were there any issues which directly influenced your life? Which issues were they? how did they influenced you
5. How would you consider using the knowledge you gained in this course in your teaching profession?
6. Do you intend to use social media in your teaching profession?
7. Are there any issues you think should be improved about this course?
8. What did you like the most in this course?
9. What was the most disliked thing about the course
10. What was the most difficult part/feature/topic about the course?
11. Is there anything else you wish to add?

D. Code Pool

Theme 1. Design Issues

Sub-theme 1. Content Related Design Issues

I. Confusing Topics
   i. Law 5651 and ISO 27000
   ii. Creative Common Types
   iii. Clickbait and Hoax
   iv. Copyright duration
   v. Copyright and Patent
   vi. Self-Plagiarism

II. Suggestions from the students
   i. Increase Technical Level
   ii. Simplify the Information Security Terms
   iii. Video and Animation can be included
   iv. Shorten the Reading Materials

v. Increase the number of examples

Sub-theme 2. Learner Related Design Issues

I. Learners' prior knowledge
   i. Nothing
   ii. Cyberethics → *Netiquette, IT use policy, freedom of speech, academic integrity, copyright*
   iii. Cybersafety → *Privacy, Fraudulent content, cyberbullying, addiction*
   iv. Cybersecurity → *Phishing and Password Protection, Virus and Protection*

II. Source of prior knowledge
   i. Daily life experience,
   ii. Special interest,
   iii. Prior schools (High school, vocational high school) or another course

III. The learners are digital natives
   i. Active and dense SNS use
   ii. The students are aware of instructional affordances of SNSs
   iii. Learners' cybersafety awareness → *Teenagers are very active in SNSs, Cyberbullying is a major concern for teenagers, Families are not aware of cyber threats through SNSs*

Sub-theme 3. Instruction Related Design Issues

I. Suggestions about instructional materials
   i. Publish Reading materials before the session

ii. Include homework or term project
iii. Include interactive activities and group work
iv. Participation in the activities must be compulsory
v. In-class participation might be balanced
vi. Duration of discussion might be controlled

II. Suggestions about the Online Environment
i. Not METUClass
ii. Not Secure
iii. Effects of the forum participation on Grading was not understood
iv. Controversial forum posts might be included
v. Instructor bias might affect
vi. Starting multiple forums discussions was the problem

III. Instruction Methods
i. Real life correspondence
ii. Different Materials, and sources
iii. Concrete Examples
iv. Critical Thinking
v. Reading Materials
vi. "First three rows" rule has a positive effect on participation

Theme 2. Challenges and Facilitators

Sub-theme 1. Facilitators for Learners

I. Direct relation to daily life
II. Duration of the course
III. The course was not too loaded
IV. Slides were sufficient
V. The content was easy
VI. Addressing all subject teachers
VII. Different Materials, and sources
VIII. Instructor's explanations with concrete examples
IX. Discussion session (Inter-dept discussions)
X. Native language support Explanation
XI. Different and Interesting topic
XII. Friendly Lecture

Sub-theme 2. Facilitators for Instructors

I. Daily life correspondence
II. Learners are digital natives

Sub-theme 3. Challenges of the Instructor

I. Students' weak reading habit
II. Technical Issues in the classroom

Sub-theme 4. Challenges of the Learners

I. Deficiency of English proficiency
II. Verbal Nature of the Course Content
III. Repetition of the topics
IV. Learning the terminology

Theme 3. Contribution of the course

Sub-theme 1. Newly Learned

Almost all of the topics, Terminology, Concepts in detail

I. Cyberethics-related newly learned
   Netizenship, code of ethics, ISO27000, Law5651, free speech, plagiarism and its types, copyright duration, DMCA, copyleft and Creative Commons
II. Cybersafety-related newly learned
   Cyber Safety, Hoax & Clickbait, Sharenting, Don't Track Act, Digital identity, Act on Cyberbullying, Addiction Stages
III. Cybersecurity-related newly learned
   CIA Triad, Phishing, Hacker Types, Malware Types, Risk and Attack Types, Mustafa Akgül

Sub-theme 2. Correcting misconception

I. Self-plagiarism does not violate academic integrity
II. Privacy settings provide privacy
III. White hat hackers are malevolent hackers
IV. Oversharing and sharenting issues
V. Digital footprint could be erased
VI. https
VII. Lack of security concern in mobile applications
VIII. 5651 based Censorship
IX. Copyleft
X. Patent Duration
XI. Types of Attacks

Sub-theme 3. Raised awareness

I. Raised Computer Security Literacy
II. Raised Awareness on Cyberethics
   i. Hate Speech
   ii. Copyright and DMCA Issues
   iii. AUP and ToS awareness
   iv. Citation and Academic Integrity
   v. Censorship
III. Raised awareness on Cybersafety
   i. Effects of Digital Footprint and PII
   ii. SNS Privacy issues

iii. Teacher Student SM Interaction issues
iv. SNS Security Settings
v. Oversharing and Sharenting
vi. Hoax & Clickbait
vii. Cyber Bullying

IV. Raised awareness on Cybersecurity
i. Cyber Security
ii. Https
iii. Phishing
iv. Hardware Security
v. Mobile Application Security
vi. Secure Password

Sub-theme 4. Perceived contribution to the teaching profession

I. Knowledge Transfer
i. Integrate into Curriculum
ii. Suggest of K12 Schools administrations

II. Aware ICT Use
i. Academic Integrity
ii. Free Speech

III. Self-Privacy Concern
i. No interaction through SNSs
ii. Special Profile or System for online interaction

IV. Students' Privacy Concern

Sub-theme 5. Direct effect on daily life

I. Benefit in another course
II. Established familiarity on Copyright issues and License Types
III. Secure surfing (https)
IV. SNSs Safety and Preserving PII
V. Self-confidence in a cyberbullying incidence
VI. Became alert in a phishing attempt
VII. Change in password management preferences
V. Started to read AUP and Terms of Service texts in an online service

E. Ethical Approval of the Study

UYGULAMALI ETİK ARAŞTIRMA MERKEZİ
APPLIED ETHICS RESEARCH CENTER

ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

DUMLUPINAR BULVARI 06800
ÇANKAYA ANKARA/TURKEY
T: +90 312 210 22 91
F: +90 312 210 79 59
www.ueam.metu.edu.tr

Sayı: 28620816 /

04 TEMMUZ 2017

Konu: Değerlendirme Sonucu

Gönderen: ODTÜ İnsan Araştırmaları Etik Kurulu (İAEK)

İlgi: İnsan Araştırmaları Etik Kurulu Başvurusu

Sayın Yrd. Doç. Dr. Cengiz Savaş AŞKUN;

Danışmanlığını yaptığınız doktora öğrencisi Evrim AKMAN KADIOĞLU' nun ***"Design and Development of an Information Security and Cyber Ethics Course for Pre-Service Teachers"*** başlıklı araştırması İnsan Araştırmaları Etik Kurulu tarafından uygun görülerek gerekli onay **2017-EGT-130** protokol numarası ile **05.07.2017 – 31.12.2017** tarihleri arasında geçerli olmak üzere verilmiştir.

Bilgilerinize saygılarımla sunarım.

Prof. Dr. Ş. Halil TURAN
Başkan V

Prof. Dr. Ayhan SOL
Üye

Prof. Dr. Ayhan Gürbüz DEMİR
Üye

Doç. Dr. Yaşar KONDAKÇI
Üye

Doç. Dr. Zana ÇITAK
Üye

Yrd. Doç. Dr. Pınar KAYGAN
Üye

Yrd. Doç. Dr. Emre SELÇUK
Üye

UYGULAMALI ETİK ARAŞTIRMA MERKEZİ
APPLIED ETHICS RESEARCH CENTER

ORTA DOĞU TEKNİK ÜNİVERSİTESİ
MIDDLE EAST TECHNICAL UNIVERSITY

DUMLUPINAR BULVARI 06800
ÇANKAYA ANKARA/TURKEY
T: +90 312 210 22 91
F: +90 312 210 79 59
ueam@metu.edu.tr
www.ueam.metu.edu.tr

Sayı: 28620816 / 197

03 Nisan 2019

Konu: Değerlendirme Sonucu

Gönderen: ODTÜ İnsan Araştırmaları Etik Kurulu (İAEK)

İlgi: İnsan Araştırmaları Etik Kurulu Başvurusu

Sayın Dr.Öğretim Üyesi Cengiz Savaş AŞKUN

Danışmanlığını yaptığınız **Evrim Akman KADIOĞLU'nun "Design and Development of an Information Security and Cyber Ethics Course for Pre-Service Teachers"** başlıklı araştırması İnsan Araştırmaları Etik Kurulu tarafından uygun görülmüş ve **2017-EGT-130** protokol numarası ile onaylanmıştır.

Saygılarımızla bilgilerinize sunarız

Prof. Dr. Tülin GENÇÖZ
Başkan

Prof. Dr. Ayhan SOL
Üye

Prof. Dr. Ayhan Gürbüz DEMİR (4.)
Üye

Prof. Dr. Yaşar KONDAKÇI
Üye

Doç. Dr. Emre SELÇUK
Üye

Doç. Dr. Pınar KAYGAN
Üye

Dr. Öğr. Üyesi Ali Emre TURGUT
Üye

F. Grading Policy and Course Outline for 2017-2018 Fall Semester – Phase 1 (1st Implementation)

Grading Policy:
- Mid-Term 1 : 25%
- Mid-Term 2 : 25%
- Participation : 10%
- Attendance : 5%
- Final : 35%

Course Outline

Week 1	First Meeting General description of information security and cyberethics
Week 2	Security Policy and Ethics Regulations • Case of Middle East Technical University • Case of Ministry of National Education
Week 3	Principle issues on information security for educators. • Use of Licensed Software • Security management of information assets • Maintenance of software and operation system
Week 4	Hardware security • Physical Security • Virus protection, • Backing up and restoring
Week 5	Identity theft • Phishing • Passwords protecting
Week 6	Ethical hacking • White-hat hackers • Social engineering
Week 7	Security issues on Mobile devices and wireless network • Critical issues on the use of Mobile devices • Trusted applications • Permissions of applications
Week 8	Security issues on Mobile devices and wireless network • Untrusted networks
Week 9	Principle issues on cyberethics in education and ethical issues on teaching activities • Netizenship • Responsibilities on students' privacy, • Online interaction issues from an ethical perspective. • Digital divide and digital equity

Course Outline

Week 10	Copyright issues, • Intellectual property, • Fair use of digital sources • Software Piracy • License Types
Week 11	Cheating and Plagiarism • Plagiarism detection software • Citation issues
Week 12	Social Media • What should teachers know about social media? • Threats, security issues and precautions on social media • Privacy issues and sharenting
Week 13	Social Media • Detection and prevention from malicious profiles • Cyberbullying and social desirability • Social Media Addiction
Week 14	Ethical issues on freedom of speech through the use of ICT • Borders and censorship • Auto-censorship • Hate speech, discrimination

G. Differences between the Course Outline and Weekly Realized Program for the First Implementation

Date	Syllabus	Realized Program
Week 1: October 6	General description of information security and cyberethics	First meeting • Course regulations and General details are presented. • A puzzle including information security and cyberethics terms is distributed. • Registration issues were explained.
Week 2: October 13	Security policy and ethics regulations • Case of Middle East Technical University • Case of Ministry of National Education	Security policy and ethics regulations • 5651 Internet Law, Article 4 • Information Technology Resources Use Policy of the university and MoNE Information Security Directive are presented.
Week 3: October 20	Principle issues on information security for educators. • Use of Licensed Software • Security management of information assets • Maintenance of software and OS	Principle issues on information security • Major terms CIA Triad • Security truisms • Risks and attack types • Hacker Types • Hardware Security tips
Week 4: October 27	Hardware security • Physical Security • Virus protection, • Backing up and restoring	Information asset types • Digital assets • Print-based information assets • Hardware assets • Soft assets
Week 5: November 3	Identity theft • Phishing • Passwords protecting	Identity theft • Phishing • Passwords protecting
Week 6: November 10	Ethical hacking • White-hat hackers • Social engineering	Security issues on Mobile devices and wireless network • Critical issues on the use of Mobile devices • Trusted applications • Permissions of applications • Untrusted networks
Week 7: November 17	Security issues on Mobile devices and wireless network • Critical issues on the use of Mobile devices • Trusted applications • Permissions of applications	Overall Review
Week 8: November 24	Security issues on Mobile devices and wireless network	EXAM

Date	Syllabus	Realized Program
Week 9: December 1	Principle issues on cyberethics in education and ethical issues on teaching activities • Netizenship • Responsibilities on students' privacy, • Online interaction issues from an ethical perspective. • Digital divide and digital equity	Principle issues on cyberethics in education and ethical issues on teaching activities • Ethics and cyberethics • Ten commandments and controversial issues • Netizenship and netiquette • Ethical Issues in Education (discussion).
Week 10: December 8, 2017	Copyright issues, • Intellectual property, • Fair use of digital sources • Software Piracy • License Types	Code of Ethics, Acceptable Use Policy • Intellectual Property • Copyright, History, First Sale Doctrine, Fair Use, DMCA • License Types and Creative Commons • Patent, Trademark • Anti-Copyright Act, Free SW, and Open SW movements • Privacy
Week 11: December 15	Cheating and Plagiarism • Plagiarism detection software • Citation issues	• Academic Integrity, • Discipline Regulations, • Honor Code, • Cheating, • Plagiarism Types • Citation issues
Week 12: December 22	Social Media • What should teachers know about social media? • Threats, security issues and precautions on social media • Privacy issues and sharenting • Responsibilities on students' privacy,	Exam 2
Week 13: December 29	Social Media • Detection and prevention from malicious profiles • Cyberbullying and social desirability • Social Media Addiction	Ethical Issues of Social Media • What should teachers know about SNSs? • Threats, security issues and precautions on social media, Fake Profiles • Oversharing • Sharenting • Teachers' Responsibilities on students' privacy,
Week 14: January 5	Ethical issues on freedom of speech through the use of ICT • Borders and censorship • Auto-censorship • Hate speech, discrimination	Ethical Issues of Social Media • Cyberbullying • Addiction • Freedom of Speech Review of the 1st and the 2nd exams

H. Summary of the Course Session Descriptions of 2017-2018 Fall Semester, The 1st Phase

1st session – October 6th, 2017

In the first meeting, a summary of the course was presented to the students. The major and most popular information security and cyberethics issues were discussed. A puzzle including the major information security and cyberethics terms was distributed to the students. The description of the course including the web site, logging procedures, grading policy, and registration procedures were also explained. The first meeting was consistent with the syllabus of the course. The students generally asked about the details on the course regulations such as attendance, grading and homework policy. They were informed that this course was the first implementation of the course and the observed findings would be used in further implementations. The students who registered to the course would be participants of the study. They were also informed about this detail.

2nd session – October 13th, 2017:

In the second session of the course, first, the terms "information" and "information asset" were explained. Later, the regulations of METU, MoNE, and ULAKBİM were presented. Also, brief definitions of the concepts of information security were also introduced to the students. This meeting was also consistent with the syllabus of the course. The brief outline included (i) 5651 Internet Law, Article 4, (ii) Acceptable Use Policy of METU, (iii) MoNE Information Security Directive, and (iv) Cyberethics. The researcher has presented the lecture.

3rd session – October 20th, 2017

In the third session of the course, the syllabus suggested to include use of licensed software, security management of information assets and maintenance of software and hardware operating systems. However, according to the researcher's lecture, the content consisted of the following subtopics: (i) Major terms, CIA Triad, (ii) Security facts, (iii) Risks and attack types, (iv) Hacker Types and ethical hackers, (v) Threats, and (vi) Hardware Security tips. The researcher decided that before explaining the basis of information security, it was not possible to explain security management, managing operating systems. Although she tried to simplify the topics covered in the course, it was

wholly related to technical details of information security. The major feedback was obtained from non-CEIT students immediately after the session. They complained about the language of the course is a highly technical level. They also claimed that the topics covered in that session were perceived to be very difficult to understand.

4th session – October 27th, 2017

In the fourth session of the course end users' role in information security was explained. Later, information assets and major precautions on those assets were presented. The major topics were listed as (i) Information security classification, (ii) Digital identities, (iii) Print-based information assets, (iv) software assets, and (v) Hardware assets.

5th session – November 3rd, 2017

This week the researcher explained digital identity, passwords, multi-level authentication strategies, and phishing concepts. The distinction between security and safety concepts was also discussed. At the end of the lecturing session, a discussion was also held. In the second hour of the session, general ethical concerns of the students were shared and discussed. As an auto critic, protection of digital identities, in particular, password strategies were also explained briefly in the previous week. This week password took more place and explained in detail. For this reason, this topic will be reorganized in the second phase of the course.

6th session – November 10th, 2017

Mobile security issues, threats, and protection ways are explained in this session. Threats to mobile security, application-level threats, and precautions, web-level threats, fake notifications, physical threats and precautions, battery safety tips, untrusted Wi-Fi, safety and privacy of data were the subtopics of the week.

In the discussion part of the session, privacy issues of the applications were discussed. When installing an application, the users approve access to many applications most of which are seem to be unnecessary. Another privacy concern of those mobile applications was that they collect our private information. The risk of a privacy breach and the benefits of those applications were compared in the discussion.

7th session – November 17th, 2017

A general summary of information security concepts was covered. In the discussion part, the students shared their different information security incidents. They also mentioned that they had been more suspicious on the internet.

8th session – First Exam, November 24th, 2017

The exam consists of 21 test questions. The questions were related to general regulations and directives, ISO-27000 standards, and major definitions, security facts, human threats, phishing, CIA triad, mobile security, untrusted Wi-Fi area. The average for the exam was 85.13. When the question-based success rates were investigated, it was seen that 14 questions of the test were answered correctly by the more than 30 students. On the other hand, one of the questions was answered wrong by nearly half of the students. It was related to the general information security standard.

9th session – December 1st, 2017

From this week and on, cyberethics issues were explained. Firstly, the terms ethics and cyberethics were covered. The most basic and brief definition of ethics is "decision between right and wrong." In some cases, to choose right or wrong may not be easy. In the lecture session, the researcher tried to show this difficulty to the students with an example; The Train Dilemma. Ten Commandments of Cyberethics and the controversial issues, Netizenship were the main topics of the week. In the discussion session, the students' different ethical concerns or decision experiences were also talked in the classroom.

10th session – December 8th, 2017

Copyright, intellectual property, and privacy issues were covered in this week. The subtopics of the course include (i) Code of Ethics, Acceptable Use Policy, (ii) Intellectual Property, (iii) Copyright, History, First Sale Doctrine, Fair Use, DMCA, (iv) License Types and Creative Commons, (v) Patent, Trademark, (vi) Anti-Copyright Act, Free SW and Open SW movements, (vii) Privacy

11th session – December 15th, 2017

Academic integrity and dishonesty were the main topics of this week. After the brief description of academic dishonesty, cheating was explained in detail. Plagiarism, prevention strategies, and detection methods were the final topics of the session.

12th session – Second Exam, December 22nd, 2017

In this exam, the major topics related to plagiarism, academic dishonesty, discipline regulations, honor code, copyright issues in the digital world were asked to students with a test. Besides, Digital Netizenship principles were asked with a matching method. As a bonus question, Mustafa Akgül was introduced to the students. The general average was 77.45. Eleven questions of the test were answered correctly by the majority, whereas the nine questions were correctly answered by the minority of the students.

13th session – December 29th, 2017

Ethical issues in social media were explained in this week. Mainly, privacy and safety issues of information sharing in social media were explained with the examples of potential harms of oversharing. Sharenting was another major topic of the week. Hoax, Clickbait, Fake identities were also covered. Lastly, the ethical behavior and interaction codes between teachers and students were discussed in the classroom.

14th session – January 5th, 2018

Cyberbullying, Addiction, and freedom of speech were the major topics of this week. Since it was the last session of the semester, all three of the topics were supposed to be explained. The researcher had two choices. She would either omit one or two of the topics and would prepare one of the topics in more detail or would cover three of the topics briefly. Since they were declared in the syllabus, the researcher decided to cover all the topics briefly. This week the exams questions were also discussed in the classroom.

Final Exam – January 12th, 2018

In the final exam all topics, with inclusion the topics of last two weeks such as ethical issues in social media, sharenting, addiction, and cyberbullying were asked in a 15 question test. The general terms in information security and cyberethics were also asked in another 25 questions matching test. General average was 86.28.

I. Grading Policy and Course Outline for 2017-2018 Spring Semester – Phase 2

Grading Policy:
- Mid-Term 1 : 25%
- Mid-Term 2 : 25%
- Participation : 10%
- Attendance : 5%
- Final : 35%

Course Outline

Week 1	First meeting • Registration issues, Course regulations, and General details. • IT Use policy and ethics regulations • Acceptable Use Policy • 5651 Internet Law, Article 4
Week 2	Principle issues on cyberethics in education • Ethics and cyberethics • Ten commandments and controversial issues • Netizenship and netiquette
Week 3	Code of Ethics and Academic Integrity • Honor Code and Discipline Regulations, • Cheating, Plagiarism Types and Citation issues
Week 4	Copyright and License Issues • Intellectual Property • Copyright, History, First Sale Doctrine, Fair Use, DMCA, DRM • License Types and Creative Commons • Anti-Copyright Act, Free SW, and Open SW movements
Week 5	*Midterm Exam 1*
Week 6	Safety Issues of the Internet • Teachers' Responsibilities on students' privacy • Interaction issues on social media • Oversharing and Sharenting
Week 7	Safety Issues of the Internet • Cyberbullying and social desirability • Addiction
Week 8	Ethical issues on freedom of speech through the use of ICT • Borders and censorship • Auto-censorship • Hate speech, discrimination
Week 9	Threats, Security issues on Digital Identities • Precautions on Social Media, Fake Profiles • Hoax and Clickbait
Week 10	• *Midterm Exam 2*
Week 11	Principle issues on information security • Major terms and CIA Triad • Security truisms • Risks and attack types • Hacker Types *Labors Day*
Week 12	Information assets

Course Outline	
	• Digital assets • Print-based information assets • Hardware assets, Hardware Security tips • Physical Security • Soft assets, Virus protection and Backing up and restoring
Week 13	Digital Identity theft • Phishing and Social Engineering • Passwords protecting
Week 14	Security issues on Mobile devices • Critical issues on the use of Mobile devices • Trusted applications • Permissions of applications

J. Differences between the Course Outline and Weekly Realized Program for the Second Implementation

Week	**Syllabus**	**Realized Program**
Week 1 February 13	First meeting • Course regulations and General details. • Registration issues. IT Use policy and ethics regulations • Acceptable Use Policy and Information Technology Resources Use Policy of the university • 5651 Internet Law, Article 4 • MoNE Information Security Directive	Description of logging issues for the course website Acceptable use policy • IT resources use Policy of the university • MoNE IT and Security Directives • 5651 Internet Law, Article 4 • Content Provides
Week 2 February 20	Principle issues on cyberethics in education • Ethics and cyberethics • Ten commandments and controversial issues • Netizenship and netiquette	• Ethics and cyberethics • Digital Citizenship and Netiquette • Digital Footprint
Week 3 February 27	Code of Ethics and Academic Integrity • Honor Code and Discipline Regulations, • Cheating • Plagiarism Types and Citation issues	Same as the syllabus
Week 4 March 06	Copyright and License Issues • Intellectual Property • Copyright, History, First Sale Doctrine, Fair Use, DMCA, DRM • License Types and Creative Commons • Anti-Copyright Act, Free SW, and Open SW movements	First sale doctrine is omitted
Week 5 March 13	Midterm Exam 1	
Week 6 March 20	Safety Issues of the Internet • Teachers' Responsibilities on students' privacy • Interaction issues on social media • Oversharing and Sharenting	Privacy, Personally Identifiable Information (PII), Non-Obvious Relationship Awareness, Oversharing and Sharenting Precautions on Social Media, Fake Profiles, Hoax, and Clickbait
Week 7 March 27	Safety Issues of the Internet • Cyberbullying and social desirability • Addiction	Teachers' Responsibilities on students' privacy Interaction issues on social media Cyberbullying and social desirability

Week	**Syllabus**	**Realized Program**
Week 8 April 03	Ethical issues on freedom of speech through the use of ICT • Borders and censorship • Auto-censorship • Hate speech, discrimination	
Week 9 April 10	Threats, Security issues on Digital Identities • Precautions on Social Media, Fake Profiles • Hoax and Clickbait	Addiction • Definition • Stages of addiction • Addiction types • Reasons and effects of addiction • Game Industry and Addiction • How to cope with addiction
Week 10 April 17	Midterm Exam 2	
Week 11 April 24	Principle issues on information security • Major terms and CIA Triad • Security truisms • Risks and attack types • Hacker Types	Same as the official
Week 12 May 8	Information assets • Digital assets • Print-based information assets • Hardware assets, Hardware Security tips • Physical Security • Virus protection and Backing up and restoring • Soft assets	Mobile related security and protection issues are added to related topics
Week 13 May 15	Digital Identity theft • Phishing • Passwords protecting • Social Engineering	Mobile related security and protection issues are added to related topics
Week 14 May 22	Security issues on Mobile devices • Critical issues on the use of Mobile devices • Trusted applications • Permissions of applications	The overall summary is presented

K. Summary of the Course Session Descriptions of 2017-2018 Spring Semester, The 2nd Phase

The 1st session – February 13th, 2018

The general course policy was introduced to the students. The course web site, instructional methods were also explained. In the lecture session, Acceptable Use Policy of the university, MoNE Security Directive for the teachers, and the Content Provider Article of the Law 5651 were constituting of the course contents. The students' concerns regarding their low level of computer literacy remained. The primary concern they presented was whether there were lab activities or not. The generic answer was that this course was generally a verbal course and there were no lab activities. However, participating in in-class activities and forums were required.

The 2nd session – February 20th, 2018

In the second session of the course mainly ethics, cyberethics, and digital citizenship (Netizenship) concepts were introduced to the students. Ten Commandments of cyberethics and the controversial issues, nine elements of digital citizenship, digital footprint, and major principles of netiquette were the subtitles.

In the discussion session of the course, Legal, Ethical and Moral concepts were compared and contradicting or supporting examples were asked to the students. The first example from the students was about child marriage. It is illegal, unethical, but it seems to be moral in rural parts of this country. The Wikipedia ban was also discussed in the classroom. The banning procedure depends on the law 5651 and legal. The lecturer asked whether it is ethical or not, whether it violates information access and free speech rights. One of the students highlighted that the being legal of banning was also unethical. Another view about Wikipedia ban was the reason for banning was not clear. Thirteen students attended the class. 5-6 students participated in discussion actively.

The 3rd session – February 27th,2018

In the third session of the course, general concepts about academic integrity, code of ethics and plagiarism were delivered to the students. The lecture outline was as consisted of the following topics (i) Code of Ethics, (ii) Academic Integrity, (iii) Honor Code, (iv) Academic Dishonesty, (v) Types and Consequences of Academic Dishonesty,

(vi) Plagiarism and types and reasons of Plagiarism, and (vii) digital cheating and plagiarism detection tools were presented to the students. Twelve students attended the class. The participation of the students was excellent. Almost all students participated in in-class discussions.

While presenting the academic- dishonesty types, co-instructor of the course gave an example for bribery as selling the registered courses in the registration period. The students complained about the registration issues and difficulties of registration to "popular" courses. Another topic which the students reacted was "self-plagiarism." It was noticed that self-plagiarism was not understood and is a common threat to academic integrity at the undergraduate level.

The 4th session – March 6th, 2018

In the fourth session of the course, intellectual property, copyright, fair use exception, DMCA and Safe Harbor provision, Creative Commons and license types, patent, trademark, Copyleft act, free and open source were presented to the students.

Since the session was the last session before the first exam, with 18 attendees, the students' concerns were mostly about the previous topics of the course. The students' contribution to the course was about patent issues, in particular, medicine patents.

The 5th session – The 1st exam – March 13th, 2018

In the fifth session of the course, the first exam covered the cyberethics concepts was done. The exam included twenty multiple choice questions with 4 points each and ten matching questions which were two points each. Multiple choice questions were evaluated the AUP, Cyberethics concepts, Copyright, Fair Use, and Safe Harbor Provision, Plagiarism, Overall average of the exam was 80.1.

The 6th session – March 20th, 2018

In the sixth session of the course, Cybersafety issues were introduced to the students. Firstly, Privacy issues with following subtopics were introduced to the students; Personally Identifiable Information (PII), Non-Obvious Relationship Awareness, potential threats and international regulations on PII, Do Not Track Statement. Later, Social Media and behavioral privacy threats, such as oversharing, sharenting were explained. The

common media literacy problems, Hoax and Clickbait were the other important topics of the session. The students' give their parents' behaviors as examples of sharenting. It was also highlighted that, a teachers' sharing their students' PII was also a sharing attitude.

Eighteen students attended the lecture. At the beginning of the session, the co-instructor asked what they know about privacy. They contributed to the legal perspective of their privacy. One of the students asked whether the authorities could be able to get their private communications in detail. A debate occurred with a side supported the legal responsibilities of the authorities and the opposing side who declared that it was a violation of private life.

The 7th session – March 27th, 2018)

In the seventh session of the course, the use of social media in education and teachers' ethical use of social media was introduced in the lecture. One of the significant threats for K12 students in the Internet era was cyberbullying. In the second part of the course, cyberbullying was also explained in detail. Types of cyberbullying, characteristic of bullies and victims were also explained in detail.

At the beginning of the session, the co-instructor asked about teachers' social media interaction with their students, whether it was a right or wrong habit. Nineteen attendees were in the class. Almost all students highlighted that it might have some negative effect on the students. They also expressed the teachers' potential privacy problems in case of an interaction with students.

The 8th session – April 3rd, 2018

Nineteen students attended the class. Freedom of speech was the main topic of the week. Symbolic Speech, Hate Speech, Censorship, Free Speech Limitations, Hate Speech, and Online Free Speech issues were the subtopics. At the end of the session, the special regulations of schools were also discussed. Free speech in other countries and Free speech issues in a school setting were this week's forum topic.

The 9th session – April 10th, 2018

In the 9th session of the course, Cyber addiction was the main topic of the week. Computer Addiction types, characteristics of computer addicted people and indicators and effects of addiction were explained. Eighteen students attended the class session.

The 10th session – April 17th, 2018

In the 10th session of the course, the Second midterm was held. The questions were related to privacy, personally identifying information, cyber addiction, and cyberbullying. The average of the exam without bonus was 91.7.

A 10-point bonus question was also asked the students, which aims at introducing four persons who have faced discrimination, violence or murder as a result of expressing their ideas. The correct answer was "All of the above." The researcher's purpose about this question was both to introduce these names and emphasize the value of the freedom of speech.

The 11th session – April 24th, 2018

In the 11th session of the course, Information security topics were introduced to the students. CIA Triad, Information Security Truisms, Vulnerability, Exploit, Threat, Impact, Risk were explained in detail. Later, threat types and human threats were clarified.

One of the major challenges, the researcher needed to handle was the lack of appropriate textbooks. The existing examples were at the expert level, and their focus varies from a holistic view, from information security management perspective to a specific detail such as risk management or network security or asset management.

Ten students attended the class. The researcher gave non-computer examples of vulnerability, risk, and threats. The majority of non-computer examples were related to security issues about banks. The common threats on Automatic Teller Machines, security breaches of POS devices, security levels of bank branches were some of the presented examples.

The 12th session – May 8th, 2018

In the 12th session of the course, information assets and precautions on assets were explained. Phishing and fake notification were also clarified. At the end of the session,

phishing activity was done. Sixteen students attended the class. The resources about asset classification and precautions were focused on financial or information systems setting. The content from the end user perspective was generally focused.

The 13th session – May 15th, 2018

In the 13th session of the course, Digital Identity, password, and malware types were the major topics of the session. Protection on digital identity and password generation strategies were the detailed subtopics. The end of the semester, students' contribution was rather low. Thirteen students attended the class.

One of the most significant contributions was related to safe password requirements. The students' had different strategies on memorizing passwords of different accounts. One of the students suggested that he set the same password for all of the accounts he signed in. Some of the students stated that, with the inclusion of two-level authentication, they were not trying to memorize the password and each time they log in a system, they generate a new password with the aid of authentication system. The risks and benefits of that strategy were also discussed in the class.

The 14th session – May 22nd, 2018

In the last session of the course, the general summary was presented. Only five students attended the class. All are contributed to the lecture. The presentation was the summary of the whole lecture contents covered throughout the semester, and the researcher tried to remind the major topics to the students. During the semester, the researcher realized that some of the topics were confused by the students. The overall brief was beneficial to correct the misconceptions. A crossword puzzle with 28 key terms was also prepared and distributed to the students in class and course web site. The puzzle is presented in Figure 4.6.

Final Exam – May 29th, 2018

In the final exam all topics, with inclusion cybersecurity-related topics of the last four weeks were asked in a 26 questions test. The researcher asked a different type of test with selections A, B, Both None. General average was 73.6.

L. A Sample Lecture Note (The First two pages)

Week 4:
Copyright and Intellectual Property

1) Intellectual property

A property (as an idea, invention, or process) that derives from the work of the mind or intellect.[1]

Digsital technologies have driven a rise in new intellectual property claims and made it much more difficult to defend intellectual property. Practically speaking, it is very difficult to protect an idea. Instead, intellectual property laws are written to protect the tangible results of an idea. In other words, just coming up with a song in your head is not protected, but if you write it down it can be protected. While protecting intellectual property is important because of the incentives it provides, it is also necessary to limit the amount of benefit that can be received and allow the results of ideas to become part of the public domain.

2) Copyright

Copyright is the protection given to songs, computer programs, books, and other creative works.

Copyright is the protection given to songs, computer programs, books, and other creative works; any work that has an "author" can be copyrighted. Under the terms of copyright, the author of a work controls what can be done with the work, including:

- Who can make copies of the work?
- Who can make derivative works from the original work?
- Who can perform the work publicly?
- Who can display the work publicly?
- Who can distribute the work?

Who owns the copyrighted book? The author or the publisher?

Many times, a work is not owned by an individual but is instead owned by a publisher with whom the original author has an agreement. In return for the rights to the work, the publisher will market and distribute the work and then pay the original author a portion of the proceeds.

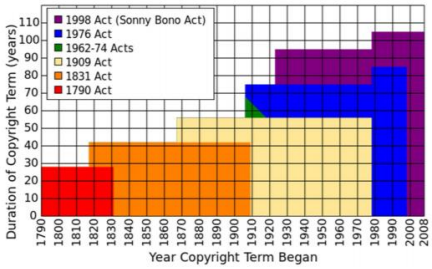
Copyright - History

The first copyright act in the world was "***The Statute of Anne***", enacted on April 10th, 1710, by British Parliament[2]. It was limited to printed books. The duration of the protection 14 years. If the author of the book was alive, copyright protection would extend 14 more years.

[1] http://www.merriam-webster.com/dictionary/intellectual%20property

[2] You can refer to http://www.copyrighthistory.com/anne.html if you interest in the first copyright act in the world, the British Statute of Anne, from 1710.

In the United States, the law was adopted in 1790, it was limited to books, maps, and charts and lasts 14 years and a 14 years renew similar to British law. Over the time, protection was expanded to include photography and motion pictures and lasts 42 years. Today; the protection lasts for 95 years from the original creation date.



Copyright – Fair Use

Fair use is a limitation on copyright law that allows for the use of protected works without prior authorization in specific cases.

Although it is generally a respected concept, the border of fair use is not clear. The following four factors are considered when determining if something constitutes fair use

1. The purpose and character of the use;
2. The nature of the copyrighted work;
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole;
4. The effect of the use upon the potential market for, or value of, the copyrighted work.

3) Digital Millennium Copyright Act (DMCA)

As digital technologies have changed what it means to create, copy, and distribute media, a policy vacuum has been created. In 1998, the US Congress passed the Digital Millennium Copyright Act (DMCA), which extended copyright law to take into consideration digital technologies.

Two of the best-known provisions from the DMCA are the ***anti-circumvention*** provision and the "***safe harbor***" provision.

- The ***anti-circumvention provision*** makes it illegal to create technology to circumvent technology that has been put in place to protect a copyrighted work. This provision includes

M. Content-Based Differences Between Two Implementations

The First Implementation	*The Second Implementation*
Intellectual Property	
Code of ethics, AUP and Privacy, were moved to different weeks. First sale doctrine, anticircumvention provision, patent, and trademark were not explained in the second implementation.	
10th week, Weekly Course Outline	***4th week, Weekly Course Outline***
Code of Ethics and AUP Copyright, History, First Sale Doctrine, Fair Use DMCA (Safe Harbour and *Anticircumvention*) *Patent, Trademark* License Types and Creative Commons Anti-Copyright Act, Free SW, and Open SW movei *Privacy*	Copyright, History, Fair Use DMCA (Safe Harbour provision) License Types and Creative Commons Anti-Copyright Act, Free SW, and Open SW movements
Addiction	
In the first implementation, it was briefly explained during the last session. In the second implementation, It was covered in detail. The topics "*Results of Addiction*" and "*Game industry and relation to Game addiction*" were added in the second implementation	
Part of 14th Week	***9th week Weekly Course Outline***
Definition Types of Addiction Avoidance Strategies	Definition and Stages of Addiction Types of Addiction *Results of Addiction* *Game industry and relation to Game addiction* Avoidance strategies

The First Implementation	*The Second Implementation*
Freedom of Speech	
In the first implementation, it was briefly explained during the last session. In the second implementation, It was covered in detail. *Speech types, symbolic speech, History of Free Speech, Limitations of Free speech, Censorship* were included in the second implementation	
Part of 14th Week	***9th week Weekly Course Outline***
Definition Article 26 Hate Speech	Definition *Speech, free speech, symbolic speech* *History of Freedom of Speech* *First Amendment in the US, Article 10 in EU and* Article 26 in Turkey *Limitations of Freedom of Speech and* Hate Speech *Censorship* *Freedom of Speech and Internet*

N. Weekly Differences Between Two Implementations

Week	Weekly Program, The 1st Implementation	Weekly Program, The 2nd Implementation
1	First meeting Course Regulations **Information Security puzzle is distributed**.	First meeting Course regulations Acceptable use policy **Security policy and ethics regulations**
2	**Security policy and ethics regulations**	**Principle issues on cyberethics in education**
3	**Principle issues on information security**	**Code of Ethics** **Academic Integrity**
4	**Protection of Information Asset**	**Intellectual Property**
5	**Digital Identity and Phishing**	**Midterm Exam 1**
6	**Security issues on Mobile devices and wireless network**	**Privacy** **Safety Issues of SNSs**
7	Overall Review	**Teachers' Responsibilities on students' privacy** **Interaction issues on social media** **Cyberbullying**
8	**Midterm Exam 1**	**Freedom of Speech**
9	**Principle issues on cyberethics in education**	**Addiction**
10	**AUP** **Code of Ethics** **Intellectual Property** **Privacy**	**Midterm Exam 2**
11	**Academic Integrity**	**Principle issues on information security**
12	**Midterm Exam 2**	**Protection of Information Assets** **Note:** Mobile related security and protection issues are added to related subtopics
13	**Ethical Issues of Social Media**	**Digital Identity and Phishing** **Note:** Mobile related security and protection issues are added to related topics
14	**Cyberbullying** **Addiction** **Freedom of Speech** Review of the 1st and second exams	The overall summary is presented **A crossword puzzle is distributed to the students**
15	**Final Exam**	**Final Exam**

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name	: Akman Kadıoğlu, Evrim
Nationality	: Turkish (TC)
Date and Place of Birth	: September 4th, 1974, Bursa
Phone	: +90 312 210 33 91
E-mail	: eakman@metu.edu.tr

EDUCATION

Degree	Institution	Year of Graduation
MS	METU Computer Education and Instructional Technology Department	2010
BS	METU Department of Mathematics	1996
High School	Bursa Girls High School, Bursa	1991

WORK EXPERIENCE

Year	Place	Enrollment
1997 August –Present	METU Computer Center	Internet Service Manager
1997 February – 1997 June	TED Ankara College – Secondary School	Computer Teacher
1996 August-1997 February	LOGO Business Solutions	Technical Support
1995 September – 1996 June	METU Mathematics Department	Student Assistant

SCHOLARSHIP

Scholar of Mathematics Department Instructors

FOREIGN LANGUAGES

Advanced English

THESES

Effect of Learning by Design Method on Student Perception in Web-Based Learning Environment – A Case Study (Supervisor: Dr. Hasan Karaarslan)

PUBLICATIONS

1. Akman, E. & Arslan, O. (2014). *Current Status in Utilization of Interactive Boards in Teacher Training Institutions* Paper presented at the 8th International Computer & Instructional Technologies Symposium, Edirne
2. Kaya, K. Y., Tisoglu, S., Ucak, S. S., & Akman, E. (2012). Perceptions of Prospective Information Technologies Teachers towards FATIH Project and Its Components. In *EDULEARN12 Proceedings* (pp. 1147-1154). IATED
3. Kaya, K. Y., Tisoglu, S., Kankilic-Ucak, S. S., & Kadıoğlu, E. A. (2012, October 4th – 6th 2012). *Investigating Technological Components of FATİH Project: A Review of Literature.* Paper presented at the 6th International Computer & Instructional Technologies Symposium, Gaziantep.
4. Akman, E., Karaaslan, H., & Uzun, F. D. (2011). *Lessons Learned from the Implementation of Learning by Design Method in a Learning Management System from the Instructor's Perspective.* Paper presented at the 5th International Computer & Instructional Technologies Symposium, Elazığ.
5. Akman, E., & Karaaslan, H. (2010). *Student Perceptions on Learning by Design Method in a Learning Management System: A Case Study.* Paper presented at the IODL&ICEM 2010, Joint Conference and Media Days, Eskişehir.

HOBBIES

Figure Skating, Gourmet, Movies, Classical music, piano