Name	Digital Citizenship Trainer Training Participant Handbook
Version	Guide, Printed Material
General Coordinator	Mustafa CANLI
Publication Coordinator	Sümeyye Hatice ERAL
Chapter Authors	Zeynep Beyza KARAKOÇ, Cem ATAY, Emine ÖZTÜRK, Gülfidan AYDIN, Kübra YİGİT, Mustafa Kemal PİŞKİNER, Neslihan YILDIZ, Raziye GÜNEŞ, Semiramis PİJNENBURG
Editors	Zeynep Beyza KARAKOÇ, Halime Gülçin BAYRAM, Neslihan YILDIZ
Project Coordinator	Zeynep Beyza KARAKOÇ
Publication Date	
Publisher Name	Ministry of National Education D.S.İ. / General Directorate of Innovation and Educational Technologies
ISBN	
License	Creative Commons License

Table of Contents

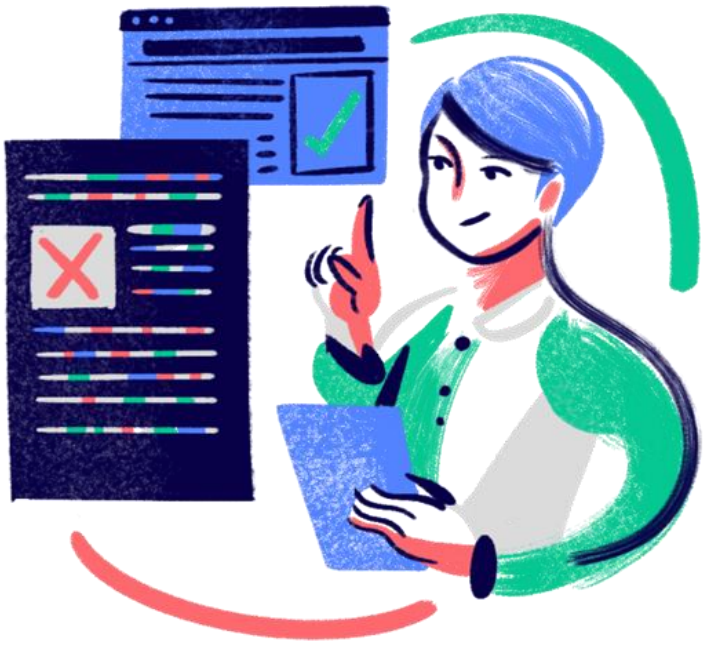
T.C. MİLLÎ EĞİTİM BAKANLIĞI
Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü

DIGITAL CITIZENSHIP EDUCATION

TEACHER TRAINER'S HANDBOOK

MODULE 1

Digital Literacy



Module

This module is a training programme that will enable trainers to gain skills in the field of digital literacy. In the digital world, it is very important that trainers have sufficient knowledge and equipment to provide students with these necessary skills. The concept of digital literacy is categorised under four headings: Information Literacy, Critical Literacy, Media Literacy and Technology Literacy. Information literacy is the ability to access accurate and reliable information sources, to evaluate and use these sources effectively. Critical literacy increases the ability to question, analyse and think critically about information and media in order to gain a critical perspective on information and media content. Media literacy includes the ability of the educator to create his/her own media content by using media tools, to understand the processes of media production, to critically analyse media content and to direct them to be conscious media users.

Learning

- To gain the ability to access reliable information in digital environments and to use this information effectively
- To develop the ability to analyse digital content from a critical point of view and to distinguish between correct and incorrect information
- To gain the skills of understanding media content correctly and using media tools effectively
- To teach how to use digital technologies in a safe, efficient and ethical way

Content Tree

Digital Literacy

1. Information Literacy
2. Critical Literacy
3. Technology Literacy
4. Media Literacy

Digital Literacy

What is Digital Literacy?

Digital literacy is a broad concept that supports individuals to access information by using digital technologies effectively and consciously, to evaluate this information correctly, to produce new content, to share this content and to use applications safely. Digital literacy enables individuals not only to use digital tools, but also to analyse the information provided by these tools, to question the sources and to use them ethically.

This module has been prepared to guide you, our esteemed teachers, in the process of teaching digital literacy skills to students. Effective and efficient use of digital tools, points to be followed in analysing the content accessed and how to access reliable sources will be emphasised. In this process, raising awareness on digital literacy, digital security and digital guidance will be prioritised.

---

1. Information Literacy

Information literacy is the ability of individuals to access information, to evaluate the information obtained and to use information effectively. In the digital world where access to information is easier, information literacy has become more important in selecting the right information and accessing reliable information. Information literacy includes not only searching for information on the internet, but also questioning, analysing and using the information found in the right context.

Being a good information literate is based on consciously managing the processes of accessing and evaluating information. Information literacy, then, is the skills of information seeking, evaluation and ethical use, offering a range of skills.

1.1. What are Information Access Methods and Information Search Strategies?

- **Information Access Methods, Information Search Strategies:** Search engines, databases and online resources, keyword selection, filtering and evaluation of results,

- **Reliability of Information:** Source reliability, scientific sources and verification methods.
- **Ethical Use of Information:** Citation rules, avoiding plagiarism and digital copyright.

- **Digital Information Resources:** Online libraries, academic databases, open access platforms.
- **Search Engine Usage:** Effective information search techniques, filtering tools and advanced search options in search engines.
- **Information Search Strategies:** Choosing the right keywords, developing targeted search strategies, understanding search engine algorithms.
- **Source Reliability Criteria:** The author of the information source, the publishing organisation, the date of the source and the validity of the references.
- **Scientific Sources and Popular Sources:** Differences between scientific sources and popular media sources.
- **Verification Methods:** Ways to check the accuracy of information, third-party verification tools (story verification sites, databases).

More than one activity option is offered in the modules, you can use the activity you find appropriate.

Acitivity

Table 1. Group work on distinguishing between real and fake news

Reliability of the source: Is the website or author publishing the news reliable?	
Headline: Is the headline sensational? Does it exaggerate to grab attention?	
Accuracy of claims: Can the content of the news be verified? Are sources cited?	
Images and videos: Check if the images used in the story are original (for example, by doing a reverse image search).	
Publication date: Is the news current or is old news being reshared?	

Participants make a credibility assessment by analysing examples from various websites and academic papers.

Review Process

Group Work: Participants are divided into small groups, each group provides the other group with two reliable and two unreliable sources to be analysed and evaluated for reliability. The groups evaluate the material. The groups start analysing the sources according to the criteria set.

Each group analyses individually according to criteria to question the level of credibility of the website/article. They can use techniques such as reverse image search to evaluate sources. This helps them to understand whether the images have been used in another context.

Presentation: The groups share their reports with the class and discuss which sources they find reliable, which sources they do not find reliable and why.

1.2. How is information organised and used?

Organising and using information requires effective information management and presentation skills in the digital age. The organisation, presentation, storage and ethical use of information is one of the cornerstones of individual and organisational success.

- **Information Management Tools:** Tools used for information organisation in the digital environment.
- **Effective Presentation of Information:** Organising and presenting information effectively, using graphs and tables.
- **Information Storage and Archiving:** Information storage and digital archive creation methods.
- **Citation Guidelines:** Using information ethically, avoiding plagiarism, citing and quoting techniques.
- **Copyright and Digital Copyright:** Copyright in the digital world, Creative Commons licences and legal regulations on the use of digital content.
- **Digital Information Sharing:** Ethical principles to be considered when sharing information, disseminating accurate information on social media and blogs.

Acitivity

Group work on the ethical use of digital content (applications of Creative Commons licences).

- Participants prepare a project using digital note-taking and knowledge management tools.
- Work on creating an effective presentation or report by bringing together different information.
- Applications are planned on the secure storage and organisation of information.

- Participants conduct research on a specific topic and apply correct citation and referencing methods.

Plagiarism control is done through sample articles, practice is done on how to prAcitivity plagiarism.

Steps

1. Introduction and Information

- **What is Creative Commons?**
  - Creative Commons (CC) are types of licences that give creators the freedom to determine how their works can be used. These licences allow copyrighted works to be shared, copied and reused by others in accordance with certain rules.
- **Creative Commons Licence Types:**
  - **CC BY (Attribution):** Content may be used with attribution to the original source.
  - **CC BY-SA (Attribution - Similar Sharing):** Content may be used with attribution as long as it is shared under the same licence terms.
  - **CC BY-ND (Attribution - Not Derivable):** Content may be used with attribution, but modification is not allowed.
  - **CC BY-NC (Attribution - Non-Commercial):** Content may be used with attribution but may not be used for commercial purposes.
  - **CC BY-NC-SA:** May be used for non-commercial purposes with attribution and must be shared under the same licence terms.
  - **CC BY-NC-ND:** Content may be used for non-commercial purposes, unmodified and with attribution.

Acitivity

Group Work

Trainees are divided into small groups of 3-4 people. Each group is given one or more examples of digital content (images, videos, articles, etc.). These contents should have different CC licences. The groups are asked to examine the Creative Commons licences of the given content and discuss how they can use the content in line with these licences.

Tasks:

- Identify which Creative Commons licence the content is under.
- Analysing the terms of the licence: Where and how can this content be used?
- Discuss how content can be shared or reused ethically and legally.
- Example: How would you use a CC BY-SA licensed image in a blog post? Where would you need to give credit?

Application and Discussion

After discussing how the given contents should be used according to their licences, the groups present their own examples of ethical ways of use to the class. During the presentation:

- They explain which Creative Commons licence they have identified and what it means.
- They express their views on how they can use the content.
- Discuss how Creative Commons licences beneficial for content producers and users.

Acitivity

Practical Use of Creative Commons Licences

Ask groups to create their own content and add an appropriate Creative Commons licence to it. For example, students could create a photo, video or article and choose an appropriate Creative Commons licence for their content.

Questions: Which CC licence did they choose and why? How do they want their content to be used?

The table below is designed to make the process of accessing, evaluating and using information in an ethical way more conscious. Your students can use this table when they are unsure about how to analyse the reliability and accuracy of information collected by an individual or group. The chart can be printed out and posted in a visible place in the classroom.

Step	Question	Control
Access to Information	Did I use the right search terms? Did I have access to reliable sources of information?	
Evaluating Knowledge	Have I questioned the information I have obtained? Have I analysed it sufficiently?	
Checking the Reliability of the Source	Is the author and organisation providing the information reliable?	
Evaluating the timeliness of information	Is the information up to date? Is it old or outdated?	
Cross Weld Control	Have I compared the information with different sources? Did I verify?	
Questioning the Impartiality of Information	Is the information impartial or does it serve the interests of a particular ideology or group?	
Ethical Use of Information	Have I used the information in an ethical way? Have I respected the labour of others?	
Correct Citation and Referencing	Have I quoted and cited correctly? Have I avoided plagiarism?	
Organising and organising information	Have I organised the information in an orderly and systematic way?	

2. Critical Literacy

Critical literacy is an important skill that defines the ability of individuals to question, analyse and critically evaluate the information they encounter in digital and printed environments.

2.1. What is Critical Thinking and What are Inquiry Skills?

Critical thinking is the ability of individuals to evaluate, analyse, interpret and reason about information to reach the right conclusions. This skill is vital to distinguish misleading and false information, especially in the digital information age.

- **Fundamentals of critical thinking:** Questioning information, developing alternative perspectives.
- **Questioning the source and accuracy of information:** Who says it? Why is he/she saying it? How reliable is what is said?
- **Be alert to bias and misleading information:** Develop awareness of ideological or emotional manipulation when disseminating or analysing information.
- **Question asking techniques:** Which questions to ask in order to analyse information in depth.

Acitivity

Participants are divided into groups of 3-4 people and take a specific media content and try to find elements of bias, incomplete information and manipulation in the content. They analyse the common points and contradictions of the content by comparing content from different perspectives.

2.2. Information Manipulation and Disinformation

The spread of misinformation is an important problem that makes it difficult for individuals and societies to access reliable information on digital platforms. Under this heading, the basic concepts of information manipulation and misinformation, how such information is disseminated and verification methods are discussed.

- **Types of misinformation:** Disinformation (deliberately spreading false information), manipulation, incomplete information.
- **The spread of misinformation in digital environments:** The dynamics of misinformation dissemination on platforms such as social media, blogs and forums.
- **Clickbait and fake news:** Detection of misleading headlines and content.
- **Verification methods:** Use of story verification sites and verification tools.

Acitivity

- Participants analyse examples from various news and content platforms and try to identify fake news.
- They work on information that spreads rapidly on social media and investigate the accuracy of this information by cross-source checking.

2.3. Analysing Media and Ideological Messages

Media literacy is the ability of individuals to analyse, evaluate and consciously consume media content. In order to develop a critical perspective, we should pay attention to the following points.

- **Media literacy and critical perspective:** Factors to be considered in the analysis of media content.
- **Media manipulation techniques:** Visual and linguistic manipulations, misleading language used in news.
- **To distinguish ideological messages:** Analysing the ideological interests behind the content in the media.
- **Social messages and stereotypes:** Analysing the stereotypes and messages imposed by the media on society.

Acitivity

- By comparing news and content from different media channels, it is discussed which messages are ideological or biased.
- Participants analyse the language and visuals used in media content and examine possible manipulations and biased messages.

2.4. Critical Literacy

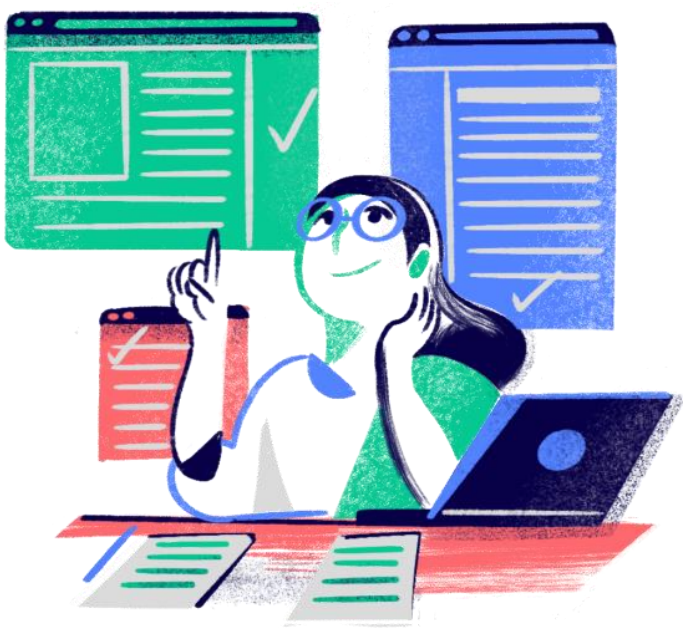
- **Contribution to critical thinking in society:** Contributions to society as a critical thinking individual.
- **Social media literacy:** Analysing social media content, sharing accurate information on social media.

Acitivity

- Participants share their critical thoughts by analysing the content of current events they encounter on social media.
- Discussions on digital ethics and responsible citizenship are carried out with group work.

Critical Literacy (How Should I Question?)

Situation: Imagine that you are following the same political event from two different news sources. The critically literate person recognises that the sources see things from different perspectives and knows that both sources represent their own perspectives, aiming to avoid echo chambers.	**Question:** What is the point of view of the person or organisation presenting the news item? What are the attitudes of this person or organisation on similar issues?
Situation: Quotations appearing on a social media platform, purporting to be from a well-known person. The critical literate person looks for sources to find out whether the quote is true or not.	**Question:** Is this content accurate? Is the source of the information reliable? Should I verify with alternative sources?
Situation: You are watching an advertisement on television about the miraculous effects of a skin care product. The critically literate person questions whether this product is really as effective as it claims to be and investigates the information presented in the advert.	**Question:** Is the language used in the advert realistic or exaggerated? Can I get more information about this product from unbiased sources?
Situation: A critical reader who encounters a headline such as "With this method, he became rich in five days!" does not immediately accept the headline, but seeks more information to understand whether the content is realistic or not.	**Question:** How does the title correspond to the content? Is the title used to mislead the reader?
Situation: When reading a research report, the critically literate person analyses the funders of the research, the methods used and the possible biases of the report.	**Question:** Who funded this research? Are the methods used scientific?



3. Technology Literacy

Technology literacy is the ability of individuals to use digital technologies effectively and efficiently. It is important for students to acquire this skill in order to be a successful individual in today's information age. It is important for educators to acquire technology literacy skills and to transfer these skills to students effectively. Technology literacy includes the conscious use of digital devices, software and online resources, compliance with digital ethical rules and developing digital security awareness.

3.1. Digital Security and Ethics

Digital safety and ethics encompasses the knowledge and skills necessary to enable individuals to exist safely, consciously and responsibly in the online world. In the digital age, it is vital that individuals protect their personal information, take precautions against online threats and act in accordance with ethical rules.

- **Safe Internet Usage:** Safe internet use covers issues such as protection of personal information, social media and security measures on online platforms. In this context, we can talk about the importance of two concepts in particular

  Protection of Personal Data: Sharing sensitive data such as identity information, address, telephone number should be avoided on online platforms

  Social Media Security: Basic measures include using strong passwords, protecting accounts with two-factor authentication, and adjusting privacy settings.

- **Cyber Threats:** How to protect against phishing, malware, viruses and hackers. It is emphasised how educators can convey these threats to students.
- **Digital Ethics:** Topics such as the importance of ethical rules in the online world, correct behaviour on social media platforms, digital footprint, online reputation are covered. Educators teach their students how to be a responsible individual in the online environment.

Acitivity

Digital Ethics Drama

- **Objective:** To teach the importance of behaving in accordance with ethical rules on the Internet.
- **Activity:** Participants are divided into groups and create a scenario based on a situation that could happen in online environments. These scenarios address digital world issues and ethical behaviour. Each group performs their scenario and the other participants identify and discuss unethical behaviours.

Creating Data Stories

- **Objective:** To show how powerful the data is.
- **Activity:** Participants are given anonymised data sets and asked to create creative stories using these data. This leads to a discussion on what conclusions can be drawn from the data and how these conclusions can be misinterpreted.

Acitivity

Technology Literacy Test

Easy Questions (1 point)

1. What is the best way to create a strong password?
    a) Using your name and year of birth

b) Choosing a short and easily remembered word
c) Using a mixture of letters, numbers and symbols

2. What does two-factor authentication (2FA) provide?
   a) Makes your account open to two people.
   b) Adds an extra layer of security.
   c) Increases your internet speed.
3. What is a phishing attack?
   a) Security software scans the computer
   b) Attempting to steal personal information through fake sites or e-mails similar to a real website
   c) A type of virus that causes the computer to slow down
4. How often is it safest to change a password?
   a) Not to change at all
   b) every 1 year
   c) On a regular basis, especially when there is a suspicious situation
5. What is the HTTPS protocol?
   a) Provides secure internet browsing
   b) Increases scanner speed
   c) Filters spam emails

Medium Difficulty Questions (2 Points)

1. What is the biggest security risk when using a device on an open Wi-Fi network?
   a) Decrease in internet speed
   b) Your information can be monitored by others
   c) Overheating of the device
2. What is one of the rules for creating a strong password?
   a) Using the same password for all accounts
   b) Use at least twelve characters
   c) Creating the password only in capital letters
3. What should you do before opening an email attachment?
   a) You should open it immediately to avoid wasting time.
   b) You should check whether the e-mail address is reliable.
   c) If you are interested in the subject of the e-mail, you can download and open it immediately.
4. What is the safest way to share your location information on a social media platform?
   a) Always keep your location open
   b) Sharing only when necessary with people you trust
   c) Keeping your location secret at all times
5. How do you know if a computer is infected with malware?
   a) The computer starts to work more slowly.
   b) Frequently appear unwanted pop-up windows.
   c) All

Difficult Questions (3 Points)

1. What is the most effective way to protect yourself from a phishing attack?
    a) Not to open e-mails from unknown persons
    b) Restarting your computer regularly
    c) Keep the security software on your computer up to date
2. What does a password manager do?
    a) Allows you to easily remember all your passwords.
    b) Creates strong passwords and securely stores these passwords.
    c) Increases computer speed.
3. Which of the following situations is one of the ways a malicious software (malware) can be transmitted?
    a) Downloading a file from an unreliable website
    b) The computer is running for a long time
    c) Leaving the Internet on all the time
4. What occurs if a computer has ransomware (ransomware) on it?
    a) Your computer suddenly switches off.
    b) Files on your computer are encrypted and you are asked to pay money to decrypt them.
    c) Your computer's processor burns out.
5. What is the Dark Web?
    a) A part of the Internet that is not accessible to the general public
    b) It is a network that provides fast internet connection.
    c) It is the name of computer networks all over the world.

3.2 Data Management and Cloud Technologies

- **Data Security:** It refers to the secure storage and backup of personal data. Ways to securely store and encrypt data in the cloud environment are explained.
- **Cloud Technologies:** Educators learn how to use cloud services such as Google Drive, OneDrive, Dropbox. They are also shown how cloud systems can be used for student projects, file sharing and collaboration between teachers.

3.3. Digital Communication Tools

Digital communication tools play a fundamental role for information sharing, collaboration and effective communication in modern education and business. However, the efficient and safe use of these tools is only possible by developing the digital skills of individuals.

- **Email Usage and Security:** Includes professional email writing guidelines, email security (spam, phishing emails) and email management.
- **Online Meeting Tools:** Demonstrates how to use online meeting tools such as Zoom, Microsoft Teams, and how to manage these platforms to increase efficiency in distance education.
- **Social Media Usage:** Information on how to use social media platforms in education, sharing information with students and safe use of social media is presented.

4. Media literacy

Media literacy is an important competence that develops individuals' ability to understand, analyse, evaluate and critically approach media content. Through media literacy, it is possible to understand how messages in digital and traditional media channels are produced, how they are disseminated and the effects of these messages on individuals. This module aims to develop participants' media literacy skills.

4.1. Understanding and Analysing Media Content

Understanding and analysing media content enables individuals to consciously evaluate media messages. Media can influence individuals' thoughts and behaviours by conveying certain messages and meanings through the language, visual elements and symbols it uses. These messages are usually shaped by editorial processes and commercial purposes. Therefore, understanding how media messages are constructed and for what purposes they are presented is a fundamental skill for critical media literacy. Analysing media content increases individuals' awareness and enables them to approach information in a more conscious and questioning way. Important concepts related to this topic are given below.

- **Media Messages:** Analysing the language, symbols and visual elements used in media content.
- **Media Production Process:** How news and media content are created, editorial processes and the commercial aims of the media.
- **Basic Principles of Media Literacy:** Learning how to read and analyse media messages.

Acitivity

- Participants analyse the subtexts and symbolic meanings of newspaper news, television advertisements and social media content.
- They analyse how a news item in different media channels is handled from different perspectives.

4.2. Manipulation Techniques Used in Media

In addition to being a powerful means of transmitting information, the media sometimes use manipulation techniques to shape public perception. These techniques include misleading language, misdirection and propaganda strategies to influence individuals' thoughts and attitudes. A common manipulation technique in the media is the distortion of images or texts. In addition, disinformation and fake news can mislead the public and lead to the spread of misinformation. The use of headlines and images to create clickbait is one of the most common attention-grabbing strategies. Being able to recognise such manipulations and critically evaluate media content is an important part of digital literacy. Important concepts related to this topic are given below.

- **Manipulation Techniques:** Misleading language, misdirection, propaganda techniques and manipulative visuals used in the media.
- **Fake News:** Recognition of fake news, techniques of spreading misinformation and disinformation.
- **Clickbait and Sensational Content:** Strategies for attracting attention through misleading headlines and images.

Acitivity

- Participants take examples from various media contents and identify the elements of manipulation in these contents.
- They investigate whether these news are true information by studying fake news samples.

4.3. Digital Media and Social Media Literacy

Digital media and social media have become one of the most common ways of information exchange in today's society. However, the functioning and content dynamics of these platforms can make it difficult for users to access accurate information. While social media algorithms recommend content based on users' interests, they can also pave the way for the spread of information pollution and misleading content. For this reason, digital media literacy enables users to critically evaluate social media content and recognise misinformation. Digital media ethics, on the other hand, covers the responsibility to disseminate accurate and reliable information and the ethical principles that should be considered when producing and sharing content. Responsible use of social media supports individuals to be more conscious and ethical in the digital environment. Important concepts related to this topic are given below.

- **Social Media Dynamics:** The functioning of social media platforms, algorithms and content recommendation systems.
- **Information Pollution in Digital Media:** Detection of misinformation, propaganda and biased content spread on social media.
- **Digital Media Ethics:** Disseminating accurate information on social media, ethical rules to be considered during the production and sharing of digital content.

Acitivity

- Participants analyse the current content they encounter on social media and evaluate the accuracy of the content by cross-source checking.
- The effects of content produced using digital media tools on society are discussed.

4.4. Social Effects of Media Content

As an important part of social life, media has the power to shape individuals' perceptions, values and behaviours. From newspapers to television programmes, from social media to digital platforms, media has a profound impact on society both as a source of information and as a means of communication. Media content influences how individuals see the world and react to social events, and plays a critical role in the representation of cultural identities and the spread of social movements. Therefore, media literacy and critical analysis of content enable individuals to become informed and effective media consumers. Important concepts related to this topic are given below.

- **Effects of Media on Society:** The effects of media content on social perceptions, values and behaviours.
- **Media and Cultural Representation:** Stereotypes in the media, representation of cultural identities and prejudices.
- **Media and Social Movements:** The role of media in social movements and mass communication.

Acitivity

- Participants analyse various cultural representations in the media and discuss the effects of these contents on social perceptions.

- Group studies are carried out on social movements that have become widespread in social media and how these movements are handled by the media.

SOURCE

Council of Europe (2022). Digital Citizenship Education Handbook. Council of Europe Publications

Buckingham, D. (2015). Defining digital literacy-What do young people need to know about digital media?. Nordic journal of digital literacy, 10(Jubileumsnummer), 21-35.
Özden, M., Meydan, E., & Günay, G. (2024). Digital Literacy Skill Scale: Reliability and Validity Study. Educational Theory and Practice, 20(1), 38-48. https://doi.org/10.17244/eku.1359401
Bayrakcı, S., & Narmanlıoğlu, H. (2021). Digital Literacy as Whole of Digital Competences: Scale Development Study. Journal of Thought and Society Social Sciences, 3(4), 1-30. Retrieved from https://dergipark.org.tr/en/pub/dusuncevetoplum/issue/63163/945319

JISC (2014). Developing Students' Digital Literacy.Digital Capabilities Framework. Available at: https://www.jisc.ac.uk/guides/ developing-students-digital-literacy . Access Date: 01.11.2024

Üstündağ, M.T., Güneş, E., & Bahçivan, E. (2017). Turkish adaptation of Digital Literacy Scale and investigating pre-service science teachers' digital literacy. Journal of Education and Future, 12: 19-29.

MODULE

Digital Health

Module

This module focuses on the physical, mental, social and cognitive negative effects of digital technologies on individuals. Throughout the training; physical ailments caused by prolonged screen use, ergonomic working order and prevention of eye strain will be discussed. In addition, the effects of social media and digital addiction on mental health, cognitive problems such as distraction and information pollution will be examined; social problems such as social media-induced anxiety, depression and cyberbullying will be discussed. The training includes strategies for developing healthy digital habits, digital detox practices and balancing technology use to minimise these negativities.

Learning

- To learn the physical, mental and social effects of digital technologies.
- To provide suggestions to students and individuals about the protection of digital health.
- To gain awareness about digital detox and healthy digital habits.

1.1.1 1. Target

The goal of this training is to provide educators with comprehensive information on the negative effects of digital technologies on the physical, mental, social and cognitive health of individuals. By transferring this information to their communities and students, educators will be able to provide guidance to balance the effects of digital technologies and create healthy digital habits.

During the training process, participants will learn about the negative effects of digital technologies on health, as well as develop practical strategies for coping with these negative effects and preventing technology addiction.

1.1.2 2. Scope

1.1.2.1 Section 1: Physical Negative Effects Caused by Digital Technologies

1.1.2.1.1 1.1. Screen Time and Physical Health

1.1.3 Digital Eye Fatigue (Computer Vision Syndrome)

When we spend a large part of our daily lives in front of a screen, our eyes are in a constant state of unfocussing and fatigue. Looking at computers and mobile devices for long periods of time makes it difficult for the eyes to refocus regularly and causes the eye muscles to overwork. Over time, this leads to digital eye strain, known as "Computer Vision Syndrome".

More than one activity option is offered in the modules, the appropriate activity can be used.

Acitivity

Eye Exercise Bingo Game

Objective:

It aims to help students maintain eye health and teach eye exercises in a fun way.

Required Ingredients

-Bingo cards (one for each student)

-Pencil or marking tools

-A written list of exercises

-Award (a small prize, sticker, etc.)

1. Bingo Card Design:

Prepare bingo cards in the shape of a 5x5 square.

Place different eye exercises in each square.

Eye Exercise List:

Close your eyes for 1-10 seconds.

2-Follow a distant object with your eyes for 10 seconds.

3-Circle with your eyes.

4-Examine a close object for 5 seconds.

5-Eye massage.

6-Switch focus (near and far object).

7-Look in different directions with both eyes.

8-Blink (quickly for 30 seconds).

9-Move your eyes (right to left, top to bottom).

Rest your eyes for 10-5 seconds.

Bingo cards are distributed, each student is given a bingo card and a pen.

1. Game Start:

The students are shown how to do the eye exercises. Each student should choose one of the exercises from the list and do it.

2. Implementation of Exercises:

The teacher reads the eye exercises in turn. After completing the exercise, the students tick the box for that exercise on the bingo card.

3rd Bingo Ad:

Students can shout "Bingo!" when they have marked five exercises horizontally, vertically or diagonally.

It is checked whether the bingo student has completed the exercises correctly and the student is rewarded.

After the game, talk to the students about eye health. They discuss which exercises they like the most and which ones work the best.

Acitivity

Letter Hunt Game:

Letter hunt is a fun and interactive game that can help improve students' eye health.

Purpose of the Game:

It aims to increase students' attention and exercise their eye muscles.

Required Ingredients:

-letter cards or objects in different sizes and colours (e.g. cardboard letters, written labels)

-Paper and pencil (for each student)

-Timer

Preparation Phase

1- Prepare the letters (write letters such as A, B, C, D and cut them out of cardboard or thick paper. You can vary the letters by using different colours and sizes).

2 - In addition to letters, they can also use objects that represent letters (e.g. an apple for A, a balloon for B).

3-Select an area inside or outside the classroom. Letters are placed in this area. By distributing the letters, various places are chosen to find them (on the tables, on the walls, in the garden).

Game Rules

Explain to the students how to play letter hunt. Each student has to find the maximum number of letters in a given time. Students are given a certain amount of time (e.g. 5-10 minutes). They are asked to find and collect the letters within this time. Students start looking for letters in the area determined by the teacher. They can count the letters or objects they find by writing them on their papers or taking them with them. The student who finds the most letters wins.

Team Work: You can divide students into groups and let them play as a team. This improves co-operation and communication skills.

1.1.4 Ergonomics and Body Posture Disorders

The effect of computer and mobile device use on neck, back and shoulder pain:

Long-term use of a computer or mobile device can lead to neck, back and shoulder pain, especially due to incorrect posture and non-ergonomic working conditions. Continuous forward bending of the neck and rounding of the shoulders cause tension in the muscles and posture disorders. Over time, this can lead to chronic pain and posture disorders.

Ergonomic device use and correct sitting positions:

Creating an ergonomic working environment is one of the most important steps in maintaining body posture. Your chair should provide full support for your back, your feet should be fully on the floor and your knees should be at a 90 degree angle. It is also important that the screen is at eye level and the keyboard and mouse are comfortable to use. These pains can be prevented by using ergonomic mouse, keyboard and adjustable desks.

1.1.5 Physical Inactivity

The impact of prolonged inactivity (sitting, screen time) on obesity, heart disease and diabetes:

Long periods of time spent in front of digital devices greatly reduce physical activity, leading to a sedentary lifestyle. Constant sitting can negatively affect the body's metabolic functions, which can

lead to health problems such as obesity, heart disease and type 2 diabetes. In addition, muscle and joint weaknesses are also common consequences of this condition.

"Every 20 Minutes" Game

Objective: It aims to ensure that the participants move regularly during the time spent in front of the computer and to reduce the negative effects of inactivity.

How to Play

Setting a Timer: A timer is set from the computer, mobile phone (every 20 minutes).

Movement Instructions: Every 20 minutes, a list is generated indicating that you should perform a specific movement.

-1 minute standing

-1 minute slow walk

-Movements such as arm and leg stretching movements can be diversified.

When the timer rings, the movement you have specified is performed. This will be a fun break for all participants. Can be played individually or in a group. When played with a group, all participants can do the movement at the same time. This increases the motivation of moving together. Participants can add different movements over time or ask for more difficulty. Thus, the game becomes more dynamic and fun. Participants can set daily goals (e.g. a total of 100 one-legged jumps).

At the end of the game, participants can discuss how they felt during the day and which movements worked best for them. This allows them to share their experiences and increases their awareness of inactivity.

Digital solutions to increase physical activity (e.g. pedometer applications):

Digital solutions can be used to reduce inactivity and increase physical activity. Pedometer apps can help people track their daily movement goals, while regular exercise reminders and health apps can encourage an active lifestyle.

1.1.5.1 Section 2: Negative Effects of Digital Technologies on Mental Health

1.1.5.1.1 2.1. Anxiety, Depression and Digital Addiction

1.1.6 Social Media Use and Mental Health

Comparisons on social media, pressure to perfectionism and low self-esteem:

Social media platforms can create an environment where people only showcase the best aspects of their lives. This causes users to constantly compare their lives with others. These comparisons with other people's achievements, holidays, physical appearance or social lives can make people feel inadequate and under the pressure of perfectionism. Over time, this can lead to low self-esteem and a negative self-perception.

The effects of social media on anxiety, depression and loneliness:

Social media can reinforce the feeling of constantly seeking a "better" life. The necessity to be constantly online and active on social media can increase stress and anxiety levels in individuals. Moreover, when long periods of time spent on social media replace real-life social interactions, people may feel more lonely and isolated. This may lead to the emergence of symptoms of depression over time.

Fear of Missing Out: Pressure to be online all the time:

Social media can cause users to experience fear of "missing out" (FOMO). The constant sharing of new content, events and news creates anxiety in individuals about missing something at any moment. This creates pressure to be constantly online and may cause the person to spend more time in front of the screen, which increases psychological anxiety levels.

1.1.7 Digital Addiction

Addictive effects of excessive use of games, social media and mobile applications:

Social media platforms, mobile games and various apps are deliberately designed to keep users on the platform. Notifications, reward systems and social approval mechanisms lead users to become more attached to these applications. Over time, this use may become addictive and individuals may start to spend more time in the digital world by disrupting their daily activities, work or school life. This can lead to time management problems and physical and mental health problems.

Coping with addiction and digital detox:

It is important to take conscious steps to deal with digital addiction. Firstly, limiting the use of social media and digital apps and setting screen time targets can be helpful. Switching off notifications, monitoring usage times and using social media purposefully can reduce the risk of addiction. **Digital detox** is a method of resting the mind by getting away from social media and digital devices in certain periods. Individuals can reduce their addiction to technology and balance their mental health by doing digital detox for certain periods of time weekly or daily.

2.2. Sleep Disorders and Blue Light Effect

1.1.8 Blue Light and Sleep Quality

Blue light emitted from screens suppresses the melatonin hormone and disrupts sleep patterns:

The blue light emitted by digital device screens (computer, phone, tablet, etc.) is transmitted to our brain via photoreceptors in our eyes and suppresses the secretion of the hormone melatonin. Melatonin is a hormone that regulates the sleep cycle and helps the body prepare for sleep during the night. Blue light can make it difficult to fall asleep by signalling the body that it is still daytime. Therefore, spending a lot of time in front of the screen, especially before going to bed, can reduce sleep quality and disrupt the circadian rhythm and cause insomnia.

The relationship between screen time and sleep and recommendations for limiting the use of digital devices:

Research shows that people who stay in front of screens for long periods of time have reduced sleep quality and an increased risk of insomnia. Stopping the use of digital devices at least one hour before falling asleep can help minimise the negative effects of blue light. It is also possible to reduce blue light exposure by using "night mode" or blue light filter settings on devices. Thus, the eyes and brain are better prepared for sleep.

Digital Detox and Application Recommendations

Take regular screen breaks:

When you spend a long time in front of a screen, the eyes and mind can become tired. It is therefore important to take regular screen breaks . The "20-20-20" rule can help here: Every 20 minutes, rest your eyes by looking at least 20 metres away for 20 seconds. At the same time, you can reduce the

effects of inactivity on the body by standing up and stretching every few hours. These breaks provide mental refreshment and increase focus.

Develop healthy sleep habits:

One of the most important benefits of digital detox is that it helps to develop healthy sleep habits. Staying away from digital devices before going to bed is an effective method to relax the mind and prevent melatonin levels from dropping. During this time, it is recommended to read a book, meditate or prepare for sleep with calming activities in low light. Also; establishing a sleep routine and going to bed and getting up at the same time every day regulates the circadian rhythm and provides a better quality sleep.

Acitivity

Digital Detective Event

It is a game that aims to enable participants to question and research the issue of technology addiction and digital detox.

Objective: It aims to encourage participants to question their relationship with technology, the effects of digital addiction and to find solutions.

Target Audience: Participants from all age groups

Materials Required: Paper, Pencil, Timer, Poster or Whiteboard

Task Cards: Cards with different tasks (for example, "Find ways to reduce your daily screen time by 30%").

A short introduction is made about the activity. It is explained to the participants that they will take on the role of a digital detective and that they will find solutions to digital addiction by fulfilling their duties. The importance of digital addiction and detox is emphasised.

Participants are divided into groups of 4-5 people. In order for the groups to interact with each other, mixed groups from different age groups are tried to be formed.

Distribution of Task Cards:

Each group receives one or more task cards. The task cards should include various topics related to digital addiction:

- "What are the benefits of digital detox? Research it."

- "Prepare a presentation on the effects of social media."

- "Think about how you can reduce your screen time and make suggestions."

- "Discover new hobbies to reduce your use of technology."

Groups are given a certain amount of time. During this time, the groups carry out research to fulfil their task. Participants can use the internet, books or their own experiences.

Each group takes turns to share their findings and recommendations with the other groups. Presentations should last 5-7 minutes and should be followed by questions from the other groups. During the presentation, groups can use creative methods (e.g. posters, presentations or role-playing). After the presentations, a discussion among the participants evaluates the proposals of each group. Discuss which proposals were the most effective and why. Participants can be asked to share their own experiences and thoughts about digital detox.

Section 3: Cognitive and Social Impacts of Digital Technologies

1.1.8.1.1 3.1. Distraction and Focusing Problems

Multitasking and Cognitive Load

The negative effects of doing many digital tasks at the same time on attention span:

Multitasking refers to the tendency to perform multiple digital tasks at the same time and is a fairly common habit in the modern digital world. However, research shows that the human brain is unable to process such multitasking efficiently. Multitasking increases cognitive load by reducing attention span and prevents a person from fully focusing on each task. This can reduce the quality of work and increase the likelihood of making mistakes. At the same time, constant task switching leads to mental fatigue, significantly reducing productivity.

Development of attention management and deep focusing skills:

Managing attention and developing deep focus skills are important to offset the negative effects of multitasking. One of the most effective steps to improve these skills is to focus on a single task, avoiding switching between tasks, and allocating specific time frames to complete that task. Time management methods such as **the Pomodoro Technique** can help in managing attention by increasing focusing times. In addition, reducing environmental distractions and switching off device notifications during a task are steps that strengthen deep focus.

Acitivity

"Silent Mind Game"

Objective: It aims to make the participants feel the effects of digital addiction on focusing and to create an environment that will enable them to focus away from technology.

Required Ingredients:

-Small difficulty cards (with tasks that require focussing)

-Timer (optional)

-Quiet environment

1. Introduction and Preparation:

Participants are asked to switch off their phones or other digital devices completely and the devices are placed in a box. The aim of the game is to test their focus by completely disconnecting from the digital world.

2. Dealing Difficulty Cards

Each participant receives a "challenge card". The cards should contain simple but distracting tasks that require focussing. For example:

"Sit quietly and close your eyes. Focus only on your breathing and think of nothing else (5 minutes)."

"Focus on the object in front of you (for example, a pen or a table). Observe all the details of the object and do not get distracted for 3 minutes."

"Write a short story of 10 words on a piece of paper, focusing only on your story."

The duration of each card is set to 3-5 minutes.

3. Completing Tasks

Each participant is given a certain amount of time to complete the tasks on the challenge card (e.g. 3-5 minutes for each task). Participants are asked to be completely silent during this time and to focus only on the task on the card. The timer is set and at the end of the time everyone will have finished their task. After all tasks have been completed, an evaluation session is held with the participants.

Questions that can be asked:

"Did anything distract you during the task? At which stages were you distracted?"

"How did this focusing exercise make you feel?"

"Did you find it easier to focus without digital devices?"

This activity will help the participants to feel the positive effects of being away from digital devices on focusing, while at the same time helping them to focus their attention.

Information Pollution

Overexposure to information weakens the ability to analyse:

In the digital age, we are exposed to an enormous amount of information every day. However, much of this information may be unverified or inaccurate. Information pollution is the result of excessive exposure to information and undermines individuals' ability to analyse this information accurately. The constant flow of information makes it difficult for individuals to distinguish between real and fake information, which increases the risk of being misinformed. Information overload can lead to mental complexity and errors in decision-making processes.

1.1.8.1.2 3.2. Effects on Social Relations

Weakening of Face-to-Face Communication Skills

The negative effects of social media and messaging applications on face-to-face communication:

Although social media and messaging applications offer quick and easy ways to communicate, they can lead to a weakening of face-to-face communication skills. Short and superficial interactions over digital platforms can lead to atrophy of important social skills such as intonation, body language and emotional expression that people develop in face-to-face communication. Since digital conversations do not carry emotional subtleties and complex social cues, it may be difficult to establish deep bonds in interpersonal relationships. This may cause individuals to have difficulty expressing themselves in face-to-face meetings and feel deficient in social relationships.

Weakening of empathy and social skills:

The habit of being constantly online and communicating through digital platforms may weaken people's ability to empathise with others. Social media and messaging applications can shorten the processes of giving and receiving emotional feedback in interpersonal communication, which can negatively affect the development of empathy. People may find it difficult to accurately understand the other person's emotional state because they do not receive important social cues such as gestures and facial expressions in face-to-face communication. Over time, this can lead to poor social skills and disconnects in interpersonal relationships.

Cyber Bullying

Increasing cases of cyberbullying among children and youth and its effects:

Cyberbullying includes behaviours such as threats, insults, exclusion or humiliating messages through digital platforms. Social media, messaging applications and online games pave the way for the spread of cyberbullying, especially among children and young people. Cyberbullying can have serious emotional and psychological effects on victims. Individuals exposed to bullying may experience problems such as depression, anxiety, low self-esteem, loneliness and school failure. In addition, being constantly online increases the risk of inevitably facing bullying.

Strategies to combat cyberbullying:

In order to cope with cyberbullying, first of all, awareness and education are important. Children and young people should be informed about cyberbullying and the harms of such behaviours. Among the strategies to combat cyberbullying:

- **Taking Action in Case of Cyberbullying:** Individuals who are bullied should be encouraged to tell an adult, teacher or trusted person without hiding the situation.
- **Blocking and Reporting the Bully:** It is important to block the bully on social media platforms and report the situation to the platform. Most platforms offer measures such as removing bullying content and banning the user.
- **Empathy and Social Responsibility Trainings:** Empathy and social responsibility awareness should be developed in schools and communities and children and young people should be taught how to be more sensitive individuals online.

30 Acitivity

The Game: "Bullying Labyrinth"

Objective: To help participants understand the emotional impact of cyberbullying and to teach them the right and supportive behaviours to adopt in the face of bullying. In this game, participants learn how to empathise when facing bullying scenarios and how to help victims of bullying.

Required Ingredients:

Labyrinth Area: One large cardboard or a labyrinth drawn on the floor with tapes (the labyrinth shape can be large or small depending on the classroom environment).

Task Cards: Cards with cyberbullying scenarios on each card.

Support Cards: Cards filled with uplifting, reassuring messages.

Path Markers: Markers (coloured cards or small objects) to indicate the completion of each task card as you move through the maze.

A labyrinth is drawn with the paths and task stops through which the participants will pass. This maze can also be done on a large sheet of paper or cardboard if space is a problem in the classroom.

A task card and a support card are placed at each stopping point. The task cards contain bullying scenarios; the support cards contain positive and encouraging messages.

Sample Support Cards:

"It's a difficult situation, but we're here for you."

"You're not alone, don't let this bullying affect you."

"Believe in yourself, you can overcome bullying with the right behaviour."

The aim of the game is explained to the participants. Each participant takes turns to enter the maze and complete the task cards at the stops. At each stop, the participant is given a card with a cyberbullying scenario and a question. The participant should read the scenario and think about what kind of behaviour he/she should show.

Sample Mission Scenarios:

"Someone makes sarcastic comments and calls you bad names online. What would you do?"

"There is a bad rumour about a friend on social media. He needs your support. How can you help her?"

"A group is having fun excluding you while playing an online game. How would you behave in this situation?"

After responding to each scenario, the participant receives a support card and reads an uplifting message. The support cards remind them to stand strong against this kind of bullying. Each time the participants give a correct or supportive answer, they move on to the next stopping point. They can receive a reward or a token card after each correct response or suggested solution. When a wrong or bullying-encouraging response is given, a short explanation is given to share why this behaviour is wrong. For example, "This kind of response may encourage the other person, it may be better to get support or ignore it."

When the participants reach the end of the labyrinth, an evaluation is made.

Discussion Questions:

"How did it make you feel to encounter cyberbullying scenarios?"

"Have you realised how you can act when a friend is being bullied?"

"What was the most important lesson you could learn from this game?"

"How do you think you would behave if you encountered or witnessed bullying in real life?"

1.1.8.2 Section 4: Solutions and Recommendations on Digital Health and Technology Use

1.1.8.2.1 4.1. Addiction Prevention

1.1.9 Conscious Use

Methods to prevent technology addiction (screen time management, notification settings, etc.):

In order to prevent technology addiction, it is important to develop conscious usage strategies and establish a healthy balance with digital devices. **Screen time management is** one of the most effective steps that can be taken in this regard. Limiting the usage time of digital devices, setting daily screen time goals and sticking to these goals makes technology use more controlled. For this, many phones and computers offer built-in screen time monitoring and limiting features. At the same time, specific usage times can be set for applications and notifications can be received when these times are exceeded.

Adjusting notification settings is an important step to reduce the constant distraction of technology. Constant notifications from apps such as social media, email and games can cause users to spend more time on digital devices. Switching off unnecessary notifications or receiving notifications only during certain time periods can make technology use more efficient and focused. Restricting access to apps at certain times or using "do not disturb" mode to take a break from technology at certain times is also an effective way to combat addiction.

In addition to these methods, doing a **digital detox** by completely avoiding digital devices at certain times helps the mind and body to rest. Using technology in a purposeful and limited way reduces the risk of addiction and allows users to lead a more conscious and balanced life in the digital world.

1.1.9.1.1 4.2. Healthy Digital Habits

- **Digital Detox and Taking a Break:**

It is an effective method to completely step away from social media at certain intervals in order to rest the mind and reduce digital addiction. For example, we can do a digital detox by completely stopping the use of social media one day a week or in certain time periods.

- **Conscious Social Media Usage:**

Controlled use of social media, benefits and risks:

While social media offers benefits such as quick access to information, community building and entertainment, overuse can carry risks such as anxiety, depression, comparison culture and addiction. Therefore, learning how to use social media in a way that does not harm health helps users maintain their psychological and emotional balance. Healthy social media habits can be developed through awareness and boundary-setting skills.

- **Ergonomic Working and Screen Usage:**

1.1.10 Ergonomic Working and Screen Usage: How to Create a Healthy and Productive Workspace?

Ergonomic working order aims to create an environment that both protects health and increases productivity. Incorrect postures and inappropriate equipment can lead to neck, back and wrist pain, eye strain and long-term orthopaedic problems. Here are the basic steps that can be followed and what can be done to create an ergonomic working order:

1.1.10.1 *1. Correct Sitting Position*

Sitting position is very important for an ergonomic working environment. Your chair should be adjusted to fully support your back and your feet should be fully on the floor. Your knees should make a 90-degree angle and your hips should be slightly higher than knee level. The back of the chair should support your spine and have a slope suitable for the lumbar region.

What can I do about it:

- **Adjustable Ergonomic Chairs**: Ergonomic chairs adapt to different body types and working positions with height and back support adjustments.

1.1.10.2 2. Screen Height and Position

Your computer screen should be at eye level and about 50-70 cm away. Having the screen too low or too high can strain the neck muscles. To avoid straining your eyes, you should hold the screen directly in front of you and adjust the brightness settings to reduce light reflection.

What can I do about it:

- **Monitor Stands**: You can use adjustable monitor stands to bring the screen height to the correct level. This helps prevent neck pain and posture disorders.

1.1.10.3 *3. Keyboard and Mouse Layout*

The keyboard and mouse should be placed so that your elbows are at your side and at an angle of 90-100 degrees. It should be in a position that you can use without bending your wrists too much and you can provide a suitable support for your wrists to rest.

What can I do about it:

- **Ergonomic Keyboard and Mouse**: It is important to use ergonomic keyboards and mice that reduce strain on the wrist and hand muscles. Vertical mice bring the wrist position to a natural angle and provide comfort for prolonged use.

1.1.10.4 *4. Screen Light Control*

Lighting in the work area should be adequate and correct to avoid eye strain. Light shining directly on the screen can cause glare, so it is important to place your screen at right angles to the light source. You can reduce the harmful light emitted from screens by using a blue light filter.

What can I do about it:

- **Blue Light Filter and Screen Protectors**: For those who work in front of the screen for a long time, blue light filter glasses, screen protectors or screen light adjustments are effective in reducing eye fatigue.

1.1.10.5 *5. Regular Breaks*

Sitting in the same position for a long time can cause tension and fatigue in the muscles. Therefore, taking short breaks every 30 minutes to stretch improves blood circulation and prevents muscle fatigue. The "20-20-20" rule is an ideal method for those working in front of a screen: Looking 20 metres away for 20 seconds every 20 minutes reduces eye strain.

What can I do about it:

- **Timer Apps**: Timing apps can help you create a healthy work routine by reminding you to take breaks at regular intervals.

1.1.10.6 6. Adjusting the Equipment at the Appropriate Height

The layout of your workspace should ensure that all equipment is easily accessible and at the correct height. The height of your desk should be adjusted so that your shoulders are comfortable, and your keyboard, mouse and other work equipment should be in a position where your hands rest naturally.

What can I do about it:

- **Adjustable Desks:** Adjustable desks, which provide the opportunity to work standing and sitting, offer the opportunity to change position during work. This reduces back and neck pain and increases productivity.

Acitivity

Digital Eye Protection Target

Objective:

It aims to enable participants to recognise and apply digital eye protection methods.

Target Cards: Cards each containing different eye protection tips or postures (e.g. "20-20-20 rule", "correct posture", "screen distance", blue light filter applications, eye examinations, screen brightness, ambient lighting).

Shooting Materials: Paper balls, soft balls or similar shooting materials.

Target Board: A board or an area on the wall where you can place the cards.

Game Rules

Place the target cards (each with a different eye protection cue) on a board or wall. Participants are divided into groups (groups of 3-4 people). Each group takes turns shooting at the target cards using the shooting material. Allow 1-2 minutes for each shot. Each group has to explain the clues written on the target cards after shooting. For example, when they shoot at the "20-20-20 rule", they have to explain what this rule is and how it should be applied. Points are awarded for correct explanations. Additional points can be awarded according to the success rate. Each group works on different cards and tries to explain them all.

At the end of the game, the group with the highest score is declared the winner. Time is allocated for each group to share what they have learnt.

Acitivity

Ergonomics and Posture Workshop (Posture Confrontation)

Objective:

It aims to enable students to learn the importance of ergonomics and correct body posture, to gain healthy habits and to recognise posture disorders.

Required Ingredients:

-Tables and chairs (classroom or outdoor)

-Chairs of different heights

-Posters or visuals showing the correct posture

At the beginning of the activity, what ergonomics is, why correct body posture is important and the effects of posture disorders are explained. It is emphasised that body posture disorders can lead to headaches, back pain and other health problems. Students are divided into groups to make their workspaces (table and chair) ergonomic. Each group works together to adjust the correct heights of the table and chair.

Points to Consider: Check the height of the chair, back supports, feet flat on the floor.

Application: Students are shown the correct sitting and posture positions. The points to be considered for correct posture are explained (such as shoulders back, waist straight, head upright).

Each student checks his/her posture in front of the mirror or in front of his/her friends.

Acitivity

Game - Posture Confrontation:

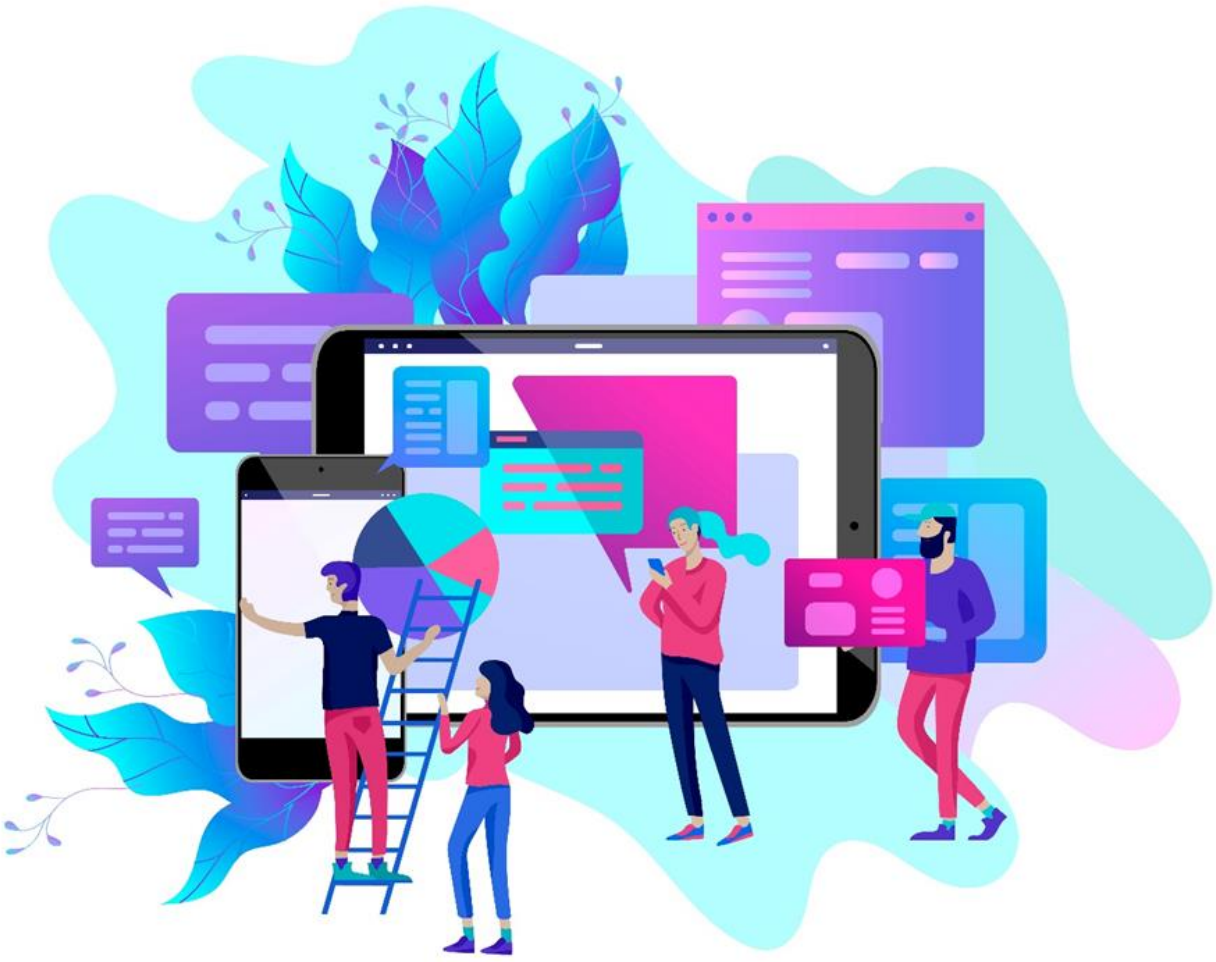
It aims to enable students to recognise and practice correct and incorrect postures.

Materials Needed: Pictures or cards showing correct and incorrect postures

Game Rules: Students are divided into two groups. Each group receives one "correct" and one "incorrect" posture card. The teacher shows the posture cards to each group in turn. The groups answer "correct" or "incorrect" according to the posture shown on the card. The group giving the correct answer should show the posture in real life. The group giving the wrong answer works together to correct the posture. At the end of the game, which postures are correct and which are incorrect and why are discussed.

MODULE

Digital Access



Module

Digital access refers to individuals' equal and active access to digital technologies (computers, smartphones, tablets, etc.) and the internet. Digital access includes not only having a physical internet connection, but also the quality, speed and security of this connection being sufficient for individuals, and the skills of individuals to use digital technologies. Digital access, which enables individuals to be included in the digital world, also enables individuals to exist and interact in digital environments.

Learning

- To recognise the work of local organisations in the field of digital access and inclusion
- To determine the strengths, weaknesses, opportunities and threats of organisations through SWOT analysis
- To gain the ability to contribute to society with digital citizenship awareness

Content Tree

What Does Access and Inclusion Mean in the Digital World?

Access to digital technology is necessary but not sufficient to be a digital citizen. The online world is a vast, limitless space full of opportunities. At the same time, it is in many ways more challenging than the offline world, especially in terms of its exponentially increasing power of diffusion, thanks to the opportunity for users to be both visible and anonymous. Digital access therefore requires not only the technical skills to effectively navigate the endless labyrinths of the online world, but also a sense of responsibility and respect for others based on the fundamental values of human dignity and human rights.

Access to technology offers new learning, communication and creative tools and platforms in all shapes and forms. These include personal or laptop computers and keyboards, mobile phones, tablets and game consoles, apps and today's robots, the internet of toys and the internet of things. One of the responsibilities of digital citizens, as in any community in which we are active, is to ensure openness to the views of minority groups, less able people and people from all walks of life in these digital spaces. This is only one aspect of the concept of "inclusion".

Today, a quarter of a century after the advent of the Internet, it is estimated that a quarter of European citizens do not have access to the Internet. When we look at the global population, this ratio indicates that almost one in two people do not have access to the internet. In many countries, it is recognised as the duty of schools to provide equal opportunities for children to realise their potential and play an active role as citizens in a digitalised world. However, in 2014, the OECD reported that only a quarter of member countries provide equal access through their education systems.

Technology is largely treated as an add-on to core curriculum subjects and digital citizenship education in schools is not fulfilling its purpose. Some countries are experimenting with Bring Your Own Device (BYOD), but this raises issues of equity and security. While inclusion is important, there is a growing realisation that neutralising poorly intended software and prying eyes is a growing challenge.

Limited educational opportunities and low income are emerging as the biggest barriers to access and inclusion in countries around the world. However, the affordability and accessibility of technology is increasing. In 2016, the number of active internet users increased by 21 per cent compared to 2015, while the number of mobile users increased by a staggering 5 per cent.

More than one activity option is offered in the modules, you can use the activity you find appropriate.

Acitivity

1. Identification of Relevant Organisations

Task: Together with the learners, create a list of relevant organisations in your community that work to ensure digital access and inclusion. These could be organisations that offer assistance with digital skills development, internet access or access to digital content.

Objective: To understand which digital access-related organisations are operating in your community and to provide a basis for analysing their impact.

2. SWOT Analysis

Task: Learners will conduct two or three SWOT analyses to evaluate the digital inclusion work of their identified local organisations. The SWOT analysis allows to assess the

strengths, weaknesses, opportunities and threats facing these organisations. In this process, choose an online tool that students can easily use.

Objective: To assess the performance of organisations through SWOT analysis and identify opportunities to improve their performance.

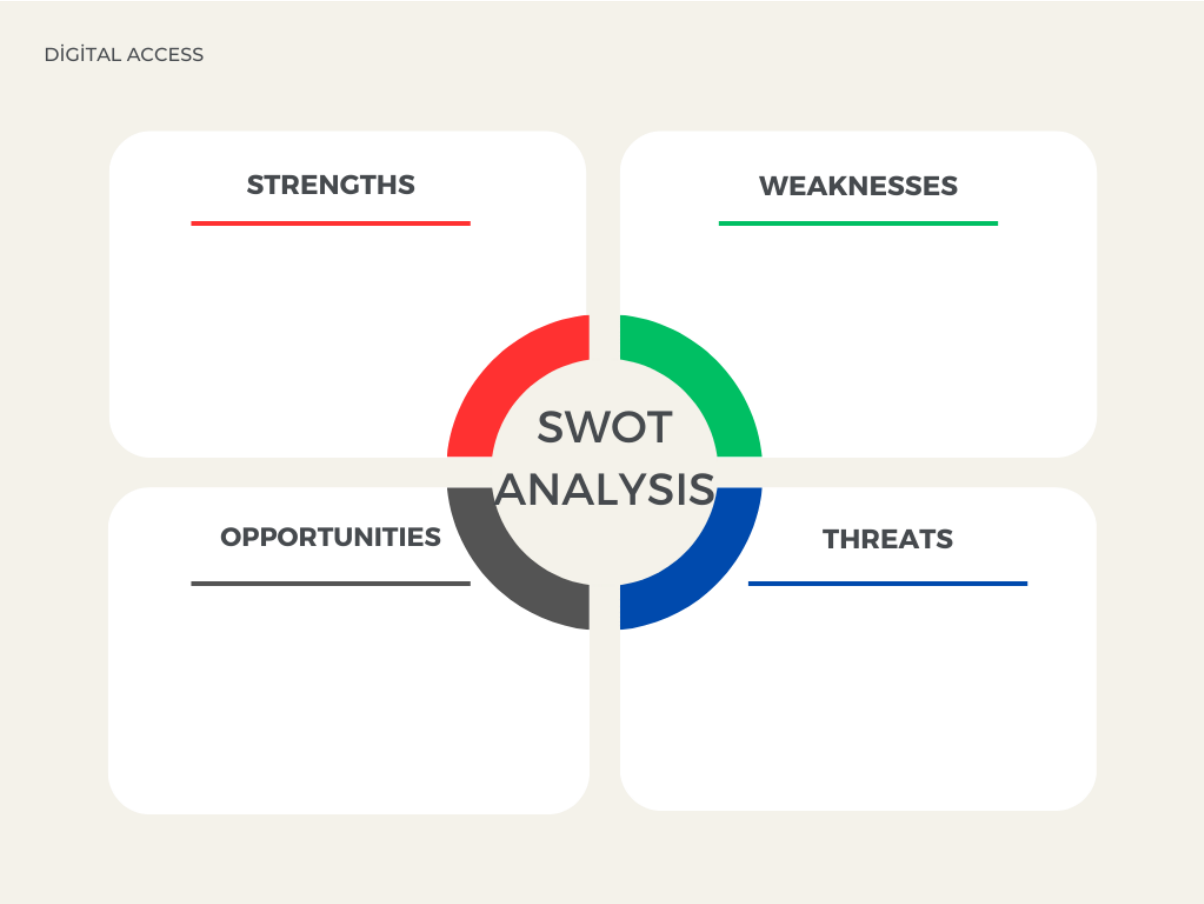


Table 2: SWOT Analysis Table

You can analyse using the table.

3. of Digital Access

Digital access refers to the ability of individuals to access digital technologies and the internet. Digital access includes not only having an internet connection but also the quality of this connection, its speed, the suitability of devices and whether individuals have digital skills.

	Physical Access: The availability of infrastructure, devices and internet services required for individuals to connect to the internet.
	Affordable Access: The cost of accessing digital devices and the internet is affordable for low-income individuals and regions.
	Social and Cultural Access: How different segments of society benefit from digital access and the impact of this access on society. Inclusion of disadvantaged groups in the digital world.
	Educational Access: Individuals learn how to use digital technologies, have digital skills and continually develop these skills.

Table 3: Different Dimensions of Digital Access

4. Discussion Questions

- Is the concept of digital access limited to the possession of technological devices, and how can we consider this concept in a broader social and economic perspective?
- What are the profound implications of unequal digital access for social justice and economic development? How can we analyse the digital divide not only as a matter of access, but also as a matter of power and influence?
- When assessing the digital access gaps and potential opportunities in your community, can you propose a creative solution to address the gaps and increase the opportunities? In particular, how can innovative ideas to increase digital literacy and access to technology be implemented?

ACTIVITY SUGGESTIONS

Digital Challenges and Competitions:

Community members are assigned specific digital tasks, such as using a service through e-government, passing an online security test, learning a digital skill (e.g. basic coding). Each time a task is completed, the group receives a point.

Digital Aid Mission: EDC Volunteers

Participants earn points by helping a neighbor who has difficulty with digital skills. For example, they can help an elderly person learn to use a smartphone, support them in completing a transaction in the e-government system, or provide information about social media account security to a friend.

Acitivity

6. Digital Access Map Preparation

- Divide the trainees into small groups (groups of 3-4 people).
- Ask each group to create a "Digital Access Map" showing how digital access is provided in their province or district. The map should include the following elements:
  - **Physical access:** Internet service providers, public Wi-Fi hotspots, libraries, internet cafes.
  - **Affordable access:** Costs of accessing devices and internet service, opportunities for low-income families.
  - **Educational access:** Local programmes for teaching digital skills, digital resources offered by schools.
  - **Barriers:** Physical, economic or social barriers (e.g. lack of infrastructure, high costs) that limit digital access in their communities.

Groups can draw their maps with coloured pencils or prepare them with digital tools.

Acitivity

7. Digital Access

Objective: This questionnaire is designed to assess the state of access to digital technologies and the internet for individuals in your community and to identify existing issues related to digital access.

1. **Do you have internet connection at home**

☐Yes

☐No.

2. How is your internet connection speed

☐Too slow

☐ Centre

☐ Fast

☐ Very fast

3. Which of the following digital devices do you have access to? (You can tick more than one option.

☐ Smartphone

☐ Computer

☐ Tablet

☐ Smart TV

Other: _____

4. Where do you usually use your digital devices

☐ At home

☐ At work

☐ At school

☐ In a library or other public place

☐ Internet cafe

Other: _____

5. How often do you use digital technologies

☐ Every day

☐ Several times a week

☐ Once a week

☐ Rarely

☐ Nothing.

6. For which purposes do you use the Internet the most? (You can tick more than one option.

☐ Social media

☐ Job and job applications

☐ Education and research

☐ Shopping

☐ Banking transactions

☐ Entertainment (films, music, games)

Other: _____

7. Do you have opportunities to develop your digital skills

☐ Yes, I attend digital skills development courses.

☐ No, I haven't got a chance.

☐ I'm learning on my own.

8. What is the biggest challenge you face when using digital devices and the internet

☐ Low internet speed

☐ Old or dysfunctional equipment

☐ Inadequate digital skills

☐ Problems in accessing digital resources

☐ Security and privacy concerns

Other:

9. Do you have any suggestions for developing your digital skills or improving your access to the internet

SOURCE

Council of Europe (2022). *Digital Citizenship Education Handbook.* Council of Europe Publications

Tonta, Y. (2002). Access to digital services and resources. *paper). PULMAN-XT Turkey National Meeting*, 16-19.

Alberta Education. (2012). Digital Citizenship Policy Development Guide. https://education.alberta.ca/media/3227621/digital-citizenship-policy-developmentguide.pdf

Beaunoyer, E., Dupéré, S., & Guitton, M. J. (2020). Covid-19 and digital inequalities: reciprocal impacts and mitigation strategies. Computers in Human Behaviour, 111, 1-9.

Aldemir, C., & Avşar, M. N. (2020). Digital Citizenship Practices in the Pandemic Period. *Journal of Eurasian Social and Economic Research*, *7*(5), 148-169.
Choi, M. (2016) A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age, Theory & Research in Social Education, 44:4, 565-607, DOI: 10.1080/00933104.2016.1210549

MODULE 4

Digital Communication

Module Scope

This module provides a comprehensive guide that examines the impact of digital communication on both personal and professional social interactions in today's technology-driven world. It examines a variety of digital communication tools and methods such as instant messaging, emails, social networks, highlighting how each method differs from traditional face-to-face interaction. Addressing the nuances of digital communication, such as the absence of non-verbal cues and the asynchronous nature of online exchanges, the module emphasises the need for users to adopt careful and effective digital practices. It also emphasises the importance of online identity, privacy and respectful participation in digital spaces as critical components of digital citizenship.

The module also covers ethical considerations for promoting a healthy digital presence, including responsible behaviour on social media and awareness of online risks such as cyberbullying and privacy violations. Through scenarios and activities, participants are encouraged to practice conflict resolution strategies and develop empathy in online interactions, equipping them with tools to constructively address misunderstandings. By integrating these principles, the module aims to foster a digital ecosystem where users are aware of the wider implications of their online actions and are able to interact thoughtfully in digital spaces, balancing connectivity with ethical responsibility

Learning Outcomes

Participants until the end of the module;

- Recognise digital communication tools (e-mail, instant messaging, social media, etc.) and understand the differences between offline and online communication.
- Manage their digital identity responsibly by understanding the importance of building an ethical and respectful digital presence online.
- Learn strategies for protecting privacy and security on digital platforms and realise the importance of protecting personal information.
- Understands the necessity of acting online in line with ethical rules and adopts appropriate communication techniques on digital platforms such as social media.
- Can manage conflict in digital environments by gaining the skills to resolve online misunderstandings, develop empathy and communicate respectfully.
- Develops careful and responsible decision-making skills by critically evaluating the effects of digital content and online behaviours.

Content

1.Introduction

1.1. Digital Communication

Digital communication has taken on an increasingly important role in both personal and professional contexts today. Characteristics specific to digital communication, such as the lack of non-verbal cues and asynchrony, markedly distinguish this form of communication from traditional face-to-face communication. These differences raise important questions about the validity of existing findings on traditional communication in the digital context and suggest the need for new research to understand the specific characteristics of digital communication processes (Strauss, Harr, & Pieper, 2024).

Communication technology now offers a wide range of tools, from the simple to the highly complex, and digital media have greatly expanded our communication capabilities. Communication has moved far beyond face-to-face and offline interactions, and a variety of forms and methods are now available in online environments. There are various methods of communication, including the following:

- **Chat:** An informal term for interactive communication in a private discussion channel in an online environment.
- **Instant messaging:** A form of real-time text communication that allows instant exchange of messages.
- **SMS:** Short message service used to send short text messages via mobile phones.
- **Emails:** Digital correspondence sent via electronic mail systems.
- VoIP (Voice over Internet Protocol): Communication via voice calls over the Internet.
- **Social networks:** Platforms that enable users to communicate and share content with large audiences.

- **Podcasts:** Pre-recorded audio content shared over the internet for streaming or downloading.
- **Virtual and augmented reality environments:** Immersive digital spaces that allow users to communicate within simulated or augmented realities.
- **Gaming platforms:** Digital environments where users interact and communicate while playing video games (Council of Europe, 2022).

As technology develops, new forms of communication such as virtual reality (VR) and augmented reality (AR) are emerging. Virtual reality (VR) allows users to interact in a digital environment where their presence is simulated in a real or imagined space. In contrast, augmented reality (AR) enhances the existing physical world by superimposing computer-generated elements, making the experience more immersive and allowing meaningful interaction.

Both VR and AR have the potential to transform the way we communicate. The immersive experiences offered by these technologies can be tailored to each individual's unique perception of reality, adding a new dimension to communication where social interactions are personalised. This means that communication can now be experienced as a customised social encounter that adapts to the different realities perceived by each participant. These advances in technology are expanding our interaction possibilities by transforming traditional forms of communication into dynamic, multi-layered experiences.

1.2. Digital Communication and Relations

In today's world, increasing technological possibilities have significantly affected how people communicate with each other. Digital platforms such as online games and social media have become an integral part of leisure activities by providing a variety of entertainment options and encouraging social interactions. However, the decrease in face-to-face interactions brings concerns about potential technology addiction (Elnur, 2023).

With the increasing presence of the Internet in our daily lives, our online identities have become more important. The way we interact with each other in digital spaces can have both positive and negative effects, affecting not only ourselves but also those around us. Creating and maintaining a healthy digital presence while communicating responsibly and without violating the rights of others is crucial to digital citizenship.

The increasing importance of online identities in the context of digital communication underlines the need for individuals to approach their virtual interactions with care and goodwill. As the boundaries between the physical and digital worlds become increasingly intertwined, our online behaviour is often a direct reflection of our personal values and affects how we are perceived in both professional and social spheres . It is important to recognise that digital interactions, like face-to-face communication, have the potential to

shape relationships, build reputations and influence others in constructive or destructive ways.

Effective digital citizenship includes an understanding of the ethical responsibilities that come with participating in online spaces. Individuals should recognise their role in promoting respectful communication, supporting inclusion and protecting the rights of others. This includes recognising the importance of privacy, intellectual property and freedom of expression, while balancing these rights with the need for responsible communication. In this context, online communication should always aim to contribute positively to the digital ecosystem, ensuring that interactions are respectful, considerate and in line with ethical standards (Council of Europe, 2022).

Maintaining a responsible e-presence involves not only being aware of the personal impact of one's digital activities, but also understanding the wider implications for society. With the proliferation of social media, online forums and digital collaboration tools, individuals are constantly communicating across geographical boundaries. Creating a healthy and constructive digital environment is therefore a shared responsibility and requires individuals to act with integrity, empathy and awareness of the consequences of their actions.

Your communication practices encompass the interactions, ideas, images, videos, and pieces of information you share with others in virtual social spaces. Naturally, these communications can take place both online and offline, and they often move between the two spaces. Interactions that begin in digital environments can influence offline exchanges, and similarly, face-to-face conversations can move to online platforms. This fluidity between online and offline communication emphasises the interconnected nature of modern interaction, where the boundaries between the virtual and physical world are increasingly blurred.

Just like e-presence, communication practices can be positive or negative. The skills needed to promote positive communication are closely linked to an individual's social and cognitive abilities in composing a message. Given the nature of online communication, where interactions can be tracked, shared and spread rapidly, often becoming popular, it is critical that digital communication makes a positive contribution to society and online communities. The potential for online interactions to reach large audiences and have long-lasting effects emphasises the importance of being intentional, ethical and socially responsible in digital spaces.

1.3. Things to Consider in Digital Communication

In the digital age, everything you upload, publish or record online leaves a digital footprint similar to footprints in the sand. This digital footprint serves as a permanent record of your

online activities and emphasises the importance of careful engagement in virtual interactions.

It is very important to think carefully before sending any message, regardless of its content. What you perceive as a positive contribution may be misinterpreted by others and lead to unintended consequences. Therefore, a critical assessment of the potential impact of your communication is extremely important.

It is also very important to protect personal information that could lead to your identification, including images that may give clues about your location or gender. Protecting privacy in the digital space is essential to protecting your identity and personal security.

Whilst it is vital to respect the equipment you use, it is also important to be aware that communications that take place over your school or employer's servers may not remain confidential. This emphasises the need for discretion and professionalism in online interactions, particularly in corporate contexts.

It is also wise to explore options that allow you to control the visibility of your online contributions. It is important to recognise that images or thoughts shared at the age of ten may evoke feelings of embarrassment when revisited at the age of sixteen. Understanding and utilising privacy settings can help to alleviate such situations and encourage a more positive online presence.

Adopting positive communication practices in the digital world is crucial to protecting personal integrity and encouraging respectful interactions. By being mindful of our digital footprints and the potential consequences of our online activities, we can contribute to a more constructive and supportive digital environment.

In today's world, digital communication enables individuals to interact with each other in innovative ways. However, despite the advantages offered by technological tools, there are also significant risks and consequences that need to be carefully assessed, for example;

- Unauthorised access to personal email accounts;
- The potential for misinterpretation of written messages, including the use of pictures, symbols and emojis;
- The widespread use of email as a method of communication by cybercriminals, including phishing, fraud and other criminal activities;
- The importance of ensuring that chat rooms are used responsibly and that discussions focus on age-appropriate topics (Council of Europe, 2022).

In terms of undesirable aspects of online communication, various negative activities can be identified in digital spaces, such as cyberbullying, online harassment, deception, cyberstalking and even avoidance of interpersonal communication.

The proliferation of these harmful practices highlights the need for greater awareness and responsible online behaviour. Online environments can facilitate anonymity, which often encourages individuals to take actions they would not undertake in face-to-face interactions. Consequently, understanding the ethical and social implications of digital communication is critical. The focus should be on educating users, especially young people, about the potential dangers and the importance of promoting respectful and responsible online interaction.

In order to develop a positive online presence, various practices can be suggested, especially in the field of digital communication:

Separate email accounts for different purposes: It is advisable to create separate email accounts for various activities, such as social media participation or online shopping. These separate accounts are not meant to be deceptive, but rather serve as a means to protect your privacy. This practice reduces the likelihood of unintended privacy breaches by compartmentalising personal and professional communications.

Adherence to online etiquette: Practising proper "internet etiquette" is crucial to promoting respectful communication in digital spaces. Whether through emails or other online platforms, it is always necessary to bear in mind that your messages can reach a wide audience. Therefore, the content and volume of your communications should be thoughtful and caring. Just as with face-to-face interactions, the tone and formality of online communication should reflect professionalism and respect for the audience.

Think before you send: Before sending an email or publishing content online, it is important to consider whether the message is something you feel comfortable saying in a public setting. The permanence of digital communication means that even private conversations can be shared and scrutinised, which emphasises the importance of deliberate and thoughtful communication in online spaces (Council of Europe, 2022).

Understand the communicative nature of online interactions: As you interact with others on various internet platforms, such as playing online games or participating in social media discussions, remember that these interactions constitute a form of digital communication. How you interact with others in these virtual environments has a significant impact on your overall digital presence. Being respectful, empathetic and considerate during these

interactions not only promotes a positive self-image, but also contributes to a healthier online community.

Creating and maintaining a positive online presence requires active participation in respectful communication, understanding the consequences of one's digital actions and protecting personal privacy. This requires balancing the benefits of connectivity with the responsibility for ethical online behaviour. As the boundaries between physical and digital communication continue to blur, the importance of fostering a constructive and respectful online presence becomes even more crucial to sustaining meaningful and positive interactions in digital spaces.

1.4. Acitivities

More than one activity option is offered in the modules, you can use the activity you find appropriate.

1. Drama Scenarios: "Digital Conflict Resolution"

Overview

In this activity, participants will simulate and role-play online conversations to practice resolving misunderstandings and conflicts effectively. By participating in these scenarios, they will develop skills in clarifying intentions and applying respectful communication techniques.

Objective:

Participants will work collaboratively to act out and analyse scenarios depicting common online misunderstandings or conflicts, developing conflict resolution and digital communication skills.

Required Materials:

- Scenario cards (pre-prepared cards with various conflict situations)

- White board and markers

Implementation:

1. Introduction: Begin by explaining the importance of communication skills in resolving online conflicts. Discuss common misunderstandings that occur in digital conversations, such as misinterpreted messages or tone. Encourage participants to consider how online interactions differ from face-to-face conversations.

2. Group Formation: Divide the participants into small groups of 4-5 people. Each group will work on a scenario card that presents a conflict situation for them to enact and resolve.

3. Scenario Assignment: Give each group a scenario card describing a specific conflict (e.g. a misunderstood message, an example of cyberbullying). Each group will read and discuss the given scenario, identify the main conflict and plan how to portray it effectively.

4. Role Play: Groups will take turns to act out their scenarios in front of the class. They will act out the conflict situation, show how the conflict escalates and then work together to resolve the conflict through effective communication strategies. Encourage participants to handle the conflict creatively and demonstrate positive interaction techniques such as clarifying tone, apologising or restating.

5. Class Discussion: After all groups have performed, lead a class discussion on the different strategies used to resolve conflicts. Analyse what worked in each scenario, discuss alternative ways of dealing with similar situations and reinforce the importance of empathy, openness and respectful language in online interactions.

Evaluation:

Participants' participation in the role-playing game will be evaluated according to their active participation, commitment to the scenario and creativity in resolving conflicts.

2. Social Media Ethics Discussion

Objective: Participants will lead a discussion about the ethical implications of social media use among young people.

Materials

- Research materials (articles, studies)

- Guide to the debate format

Implementation:

1. Introduction: "Should social media platforms be regulated to protect young users?" Introduce the topic of the debate. Explain the rules and format of the debate.

2. Research Phase: Participants will be divided into two teams (for and against) and given time to research their arguments using the materials provided.

3. Debate Preparation: Teams will prepare their opening speeches and counter-arguments.

4. Conducting the Debate: Each team will present their arguments, followed by rebuttals and closing remarks. Encourage respectful discourse and active listening.

5. Reflection: After the debate, the participants will write a short reflection on what they have learnt and how their views may have changed.

Evaluation:

Judging will be based on the quality of the arguments presented, the ability to respond to counter-arguments and overall participation in the debate.

3. Digital Citizenship Workshop

Objective: Participants will learn the principles of digital citizenship and create guidelines for responsible online behaviour.

Materials

- Digital citizenship resources (articles, videos)

- Graphic paper and felt-tip pens

Implementation:

1. Introduction: Introduce the concept of digital citizenship and its importance in today's society. Show a short video about responsible online behaviour.

2. Group Research: In small groups, participants will explore different aspects of digital citizenship (e.g. privacy, communication, online etiquette).

3. Creating Guidelines: Each group will create a set of guidelines based on their research. They will present these guidelines on graph paper.

4. Gallery Tour: The groups will display the guides they have prepared in the classroom. Participants will walk around, read each guide and give feedback or suggestions.

Evaluation:

- The evaluation will be based on the quality of the guidelines created, creativity in the presentation and active participation during the gallery walk.

4. Collaborative Infographic Creation: "Effective Digital Communication"

Overview

In this activity, participants will work together to create informative infographics on effective digital communication. They will research, design and compile an engaging guide that highlights best practices for respectful and effective online interaction. This guide will serve as a peer resource that promotes positive digital interactions and increases awareness of the nuances of communication in a digital context.

Objective:

Participants will collaborate to research and design infographics that offer key tips and strategies for effective digital communication with a focus on clarity, audience awareness and respectful language.

Required Materials:

- Computers with design software or online infographic tools (e.g. Canva)

- Access to research materials (articles, online resources on digital communication practices)

Implementation:

1. Introduction: Begin by discussing the importance of digital communication and its impact on social interactions. Explain that participants will work in groups to create an infographic that can guide their peers on how to communicate effectively in digital environments. Emphasise that their final product should be visually appealing, informative and easy to understand.

2. Research and Planning: Divide participants into small groups and assign each a different aspect of digital communication (e.g. clarity, tone, audience awareness, respectful language). Each group will gather information, including examples and best practices, with a focus on creating a short but effective infographic section.

3. Infographic Design: Participants begin to create their infographic sections using the design tools. Encourage them to think creatively about layout, colour schemes, icons and other visuals to enhance readability. Each section should include practical tips, relevant examples and a balance of text and images to clearly capture key messages.

4. Compilation of Infographics: Once the groups have completed their sections, they will come together to compile the infographics into a coherent digital guide. They can include a cover page, a short introduction and credits to recognise each group's contribution. This final product can be shared in class or used as a digital resource.

5. Presentation and Reflection: Each group presents their infographic and explains the choices they made in design and content. As a class, discuss how these strategies can enhance digital interactions and reflect on the value of visual tools in promoting understanding and awareness.

Evaluation:

Group Infographic Rubric:

- Content Accuracy (20%): Information is accurate, relevant, and clearly presents best practices in digital communications.

- Design and Visual Attractiveness (20%): The infographic is visually appealing with a balanced use of colour, symbols and spacing.

- Clarity and Readability (20%): The text is concise and easy to understand, and its logical flow facilitates comprehension.

- Creativity (20%): The group demonstrates originality in its visual designs and incorporates unique elements that make the infographic memorable.

- Co-operation (20%): Group members worked effectively together, showing evidence of balanced participation and shared responsibility.

Acitivity

5. Joint Story Writing: "Navigating the Digital World"

Objective: Participants will collaboratively write a story that explores digital communication, online interactions and their impact on personal relationships, developing awareness and critical thinking through narrative.

Materials:

- Interactive board or projector

- Story outline templates

- Thought diaries

Overview: Participants will work in groups to create a collaborative story in the context of digital communication. Each group will contribute different parts of the story and together they will create a narrative that emphasises various aspects of online interaction, including both positive and negative elements. This activity is designed to encourage creativity, teamwork and reflection on the complexity of the digital world.

Implementation:

1. Introduction and Discussion: Start with a class discussion on digital communication by asking the participants questions such as

- "What are the benefits of communicating online?"
- "What difficulties have you experienced or observed in online communication?"
- "How can online interactions affect relationships positively or negatively?"

Introduce the idea of a collaborative story in which each group of students will be responsible for writing different parts of a shared narrative.

2. Story Planning: Divide the participants into small groups of 3-4 people. The class will design a story based on the concept of a group of characters who together experience various aspects of digital communication (e.g. online friendships, misunderstandings in text

messages, a virtual collaboration project and dealing with online conflicts). Create a rough outline on the board, dividing the story into chapters.

The characters communicate in the digital world and develop their interactions by meeting each other. However, a conflict arises, such as a misunderstood message or cyberbullying, and relationships become strained. They resolve this conflict using positive communication strategies and realise the importance of being more aware and respectful in digital communication. This experience helps them to develop empathy and common sense in their digital interactions.

3. Writing a story in groups: Ask each group to write a part of the story based on the outline. Encourage participants to use real-life digital communication methods such as texting, video calls or social media posts to make the story authentic. Using a shared Google Doc or similar platform, groups can work on their chapters at the same time, recognising each other's contributions and ensuring continuity in the story. When writing, participants should consider how their characters might feel, react and communicate in each situation.

4. Compiling and organising the story: After each group has completed its part, put the story together in a single document. Read the story as a class to check for flow, coherence and consistency in character development. Make any necessary edits and encourage participants to suggest changes or additions to improve the story's message about responsible digital communication.

Class 5 Presentation: Each group will present their section of the story and explain the choices they made in terms of character actions, dialogue, and resolution. Following the reading, lead a class discussion on how the experiences of the characters in the story reflect real-life situations and how they can apply the lessons learnt to their own online interactions.

6. Reflection and Feedback: Participants will write in their diaries a short reflection on what they have learnt from the collaborative story writing experience. Guiding questions may include the following examples.

- "What surprised you about the characters' online interactions?"
- "What would you do differently in a similar digital situation?"
- "How can stories like this help us understand and improve our own digital communications?"

Evaluation:

Story Content: Evaluate the story's integrity, creativity, and portrayal of digital communication themes.

Co-operation: Observe the cooperation, communication and teamwork of the participants throughout the process.

Reflection Journals: Assess the depth of student reflections and their ability to connect events in the story to personal insights about digital interactions.

SOURCE

Council of Europe. (2022). *Digital citizenship education handbook*.

Elnur, A. (2023). The transformation of the sociology of leisure in the context of digitalisation of communication processes. *Academic Sensitivities, 10*(23), 287-311.

Strauss, C., Harr, M. D., & Pieper, T. M. (2024). Analysing digital communication: a comprehensive literature review. *Management Review Quarterly*, 1-39.

MODULE 5

Digital Commerce

Module Scope

This module is a training programme aiming to provide knowledge and skills on digital commerce. This module covers digital commerce, the potential of digital commerce, the benefits and risks of digital commerce, digital consumers. The growth of online platforms, new technologies, the production of services, the way materials and services are supplied and the way they are delivered, the change of trading activities, the emergence of new challenges and opportunities are important in today's trade.

Learning Outcomes

- Recognise digital commerce conceptually.
- To compare the growth rate of digital trade in the world and in our country.
- Raising awareness of the benefits of digital trade.
- Recognise the risks of digital commerce and learn the precautions to be taken.
- To learn the concept of digital consumer.
- To realise what needs to be done to be a conscious consumer.

Content

1.2 Expectations from the module:

- What do you expect to learn from this module?
- The participants are instructed to write their expectations on a notepaper and they are given a notepaper and asked to write their expectations.
- The papers are hung on the board for everyone to see.

1.3 Description:

Dance Movements of the Name

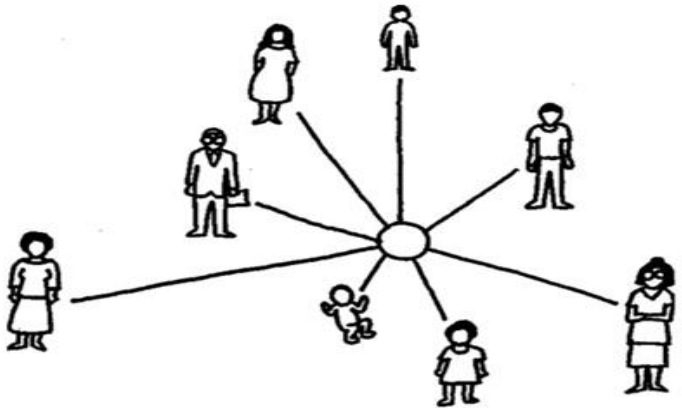
- The participants stand in a circle.
- The first participant associates each syllable in his/her name with a movement (hand or leg movements, steps, pirouettes, head movements, etc.).
- The next participant repeats the movements of the first person by name and adds his/her own movements.
- The group repeats the movements and names together.
- The game continues in this way until the last person.

1. Digital Commerce

With the rapid development of communication technologies and the Internet, a new and different economic order has emerged. With these changes, geographical borders have been removed, markets have gained a different dimension and sellers have seen the whole world as potential customers and carried their commercial activities to web-based systems (Civan and Bal, 2002: 1011). Digital networks have brought a new dimension especially to the field of trade. These networks reduce search costs by enabling buyers and sellers to connect more quickly and easily. In addition, communication and coordination costs can also be reduced, which contributes to lower transport costs (Abeliansky and Hilbert, 2017).

Digital commerce refers to a broad area covering the buying, selling and ordering of goods and services over the internet. According to the World Trade Organisation, digital trade is the production, distribution, marketing, sale or delivery of goods and services to buyers by electronic means. In this context, digital commerce includes not only shopping transactions, but also processes such as marketing, customer support and commercial communication. These activities, which are carried out through computer networks, allow trade on a global scale to be carried out more quickly, effectively and comprehensively (Civan and Bal, 2002: 1011).

1.1. Scope of Digital Trade



The general scope of e-commerce, which means commercial transactions (shopping) via the Internet, includes all organisations, whether for profit or not. From this point of view, the general framework of e-commerce can be made as follows (Elibol and Kesici, 2004, p. 306).

- Buying and selling digital content or physical goods,
- Marketing of products to consumers without using any intermediary,
- Promotion, advertising and information activities,
- Transactions and contracts between commercial organisations,
- After-sales support and making tenders in electronic environment,
- Performing electronic bank transactions,
- Joint design and production projects,
- Keeping and monitoring business records,
- Delivery of digital content,

- Utilisation of public and private sector services.

However, the scope of e-commerce is not limited to shopping through the internet. In general terms, e-commerce includes activities such as producing, selling, advertising, advertising, providing after-sales technical support and making payments through computer networks (Kaya, 2002 cited in Özel, 2013, p. 2).Bucaklı (2007) lists the scope of e-commerce as follows:

- Digital exchange of goods and services,
- Production planning, organisation and supply chain creation,
- Promotion, advertising and information activities,
- Order creation processes,
- Processes of making agreements,
- Electronic bank transactions and fund transfers,
- Electronic bill of lading submission,
- Customs clearance procedures,
- Public procurement in electronic environment,
- Transactions made by electronic mail,
- Electronic share exchange and stock exchange transactions,
- Keeping and monitoring business records,
- Direct to consumer marketing activities,
- Transactions such as digital signature, electronic notary,
- Instant distribution of digital content,
- Instant information creation and transfer,
- Taxation in electronic environment,
- Transfer of intellectual property rights,
- Production monitoring in digital environment,
- Shipment tracking in digital environment.

1.2. Digital Trading Tools

In general, all kinds of technology and technology products that facilitate the transactions of parties engaged in commercial activities can be defined as electronic commerce tools. These

tools include internet, computer, tablet, fax, telephone, electronic data interchange (EDI) systems and electronic payment systems. The most commonly used e-commerce tools are electronic data interchange systems, internet networks and electronic payment systems (Arpacı & Uluçay, 2012; cited in Akçi & Göv, 2015, p. 415).

1.4 1.3. Types of Digital Trade

E-commerce is generally categorised as direct and indirect e-commerce. In indirect e-commerce; the sellers advertise the products, the goods are examined by the customers, the order is created electronically, but the physical delivery is made in traditional ways through postal service or commercial couriers. Direct e-commerce, on the other hand, includes computer programmes, audio-visual goods and services with entertainment and cultural content, where the ordering, payment and delivery processes are carried out entirely digitally (Özel, 2013, p. 4).

2. The Potential of Digital Trade

Today, in the period called the Information Age, the rapid spread of computers and the Internet has deeply affected trade and led to the emergence of e-commerce as an alternative and innovative alternative to the traditional understanding of trade. In this context, e-commerce can be seen as a new trade model associated with the globalisation process (Özdemir, Törenli and Kıyan, 2010). One of the most important innovations that distinguishes e-commerce from traditional trade is that it enables shopping at any place and time by eliminating the space and time restrictions of commercial activities (Akçi & Göv, 2015, p.412). In this way, e-commerce, which facilitates the purchase and sale of goods and services that take place face-to-face in traditional processes, has become increasingly widespread, especially with the advances in internet technology (Kayahan & Hepaktan, 2016, p.160).

30 **Size of Digital Trade**

- Participants are divided into two groups.
- The first group researches the size of digital trade in the world between 2014 and 2024 using digital tools, prepares a report and makes a presentation.
- The second group researches the size of digital trade in Turkey between 2014 and 2024 using digital tools, prepares a report and makes a presentation.

1.5 2.1. Digital in the World

Digital trade stands out as a new trend in foreign trade today and provides significant gains especially in countries such as the USA. Studies show that the Internet has had a great impact on foreign trade since the late 1990s (Artan and Kalaycı, 2009, p. 181). According to current economic data, the share of e-commerce volume in total trade volume is increasing day by day (Yeniçeri, 2008). E-commerce provides time and cost savings to both sellers and buyers and also provides advantages such as increased productivity. In addition, it offers firms (organisations or businesses) the opportunity to do business on a global scale (within the scope of the whole world) (Artan & Kalaycı, 2009, p.176). Thanks to the Internet, firms can operate worldwide with lower costs and without facing market entry barriers, while consumers have the opportunity to access a wider variety of goods and services without the

need for intermediaries (Özel, 2013, p. 2). Regardless of the size of a firm operating on the Internet, its field of activity is now the whole world (Elibol & Kesici, 2004, pp. 204-304).

With the start of the pandemic process, e-commerce in the world has entered a rapid growth and development process. While the global e-commerce volume was approximately 5.5 trillion dollars in 2022, it grew by more than 25% in 2023, reaching approximately 7 trillion dollars.

1.6 2.2. Digital Trade in Turkey

Today, both the public and private sectors in Turkey have made significant progress in providing services over the internet. The proportion of enterprises with internet access increased from 80.4 per cent in 2005 to 90.9 per cent in 2010, which is an indication of the rapid adaptation of entrepreneurs to the internet (Özel, 2013, pp. 13-14). This situation indicates that the volume of e-commerce is growing exponentially every year. For economic units, the Internet has become a necessity rather than a preference or adaptation to technology (Kayahan & Hepaktan, 2016, pp. 185-186). Despite this, internet usage in Turkey is progressing faster than e-commerce and it is known that e-commerce has not yet reached the expected level in Turkey. Currently, there are around 12,000 e-commerce websites in Turkey. While the volume of e-commerce in Turkey was 600 billion Turkish Liras in 2022, it exceeded 850 billion Turkish Liras in 2023. It is thought that the share of global e-commerce in total retail sales has exceeded 21% and this rate will exceed 25% in a few years and may reach 50% in the next 5-10 years (2023 target, 2023).

Banks offering services over the Internet are pioneering in this field by improving their websites day by day (Küçükyılmazlar, 2006, pp. 35-37). In addition, bookstores, CD sellers, electronic and computer parts sellers and toy shops also play a leading role in the development of e-commerce in Turkey. Another digital area that has developed thanks to e-commerce is the buying and selling of tickets. Today, more than 70 per cent of ticket buying and selling transactions used for various purposes are carried out online (Arslandere, 2010,

p.53-54). In Turkey, with the strengthening of the legal infrastructure for the restructuring of the telecommunication structure within the framework of e-commerce, e-commerce is expected to expand further. The first comprehensive study on e-commerce was the establishment of the Electronic Commerce Coordination Board (ETTK) in 1998. Later on, this board was named as e-Commerce Board (ETİK). In 2003, e-Documentation in Foreign Trade and e-Financial Services group was established and "Internet Supreme Board" can also be counted within this scope (Küçükyılmazlar, 2006, pp. 35-37).

According to the Deloitte report, retail e-commerce sales figures worldwide between 2014 and 2019 are as follows:

- 1.336 trillion dollars in 2014,
- In 2015, it was $1.548 trillion,
- In 2016, it was $1.845 trillion,
- In 2017, it was $2.382 trillion,
- In 2018, it was $2.982 trillion,
- In 2019, $3.535 trillion.

Select Symbol

- Participants are told that they are a seller who trades on the internet. They are asked to create symbols of their company on the computer to increase their sales. Symbols are discussed with the group.

1. Do the symbols represent the values of the companies?

2.Does it create a sense of shopping in the customer?

3. Does it inspire confidence?

4. Does the company provide information about the products/services it sells?

1.7 3. Benefits and Risks of Digital Trade

Discussion Programme

- Participants are divided into two groups.
- They are told that they have been invited to a discussion programme on television.
- Groups are given topics.
- The first group advocates the benefits of digital commerce/shopping.
- The second group defends the risks of digital trade/shopping and traditional trade/shopping.
- Groups are given 5 minutes to prepare.
- A volunteer participant hosts the discussion programme.

1.8 3.1. Benefits of Digital Trade

Thanks to the Internet, consumers have the opportunity to shop twenty-four hours a day, every day of the year. In addition, they have the opportunity to purchase goods and services at lower prices, to access digital products such as software more easily and to make barter among themselves worldwide. The benefits of e-commerce for consumers can be listed as follows (Doğaner, 2007: 35-36):

- It offers the opportunity to see the products, review and shop without leaving home.

- Reduces transport costs.
- It provides the opportunity to see the product range more easily.
- In online retailing, effective product presentation facilitates consumers' decision-making processes by increasing the attractiveness of the web page (Yoo & Kim, 2014; Algharabat, 2014; Ozok & Komlodi, 2009;Algharabat et al., 2017).

In the process of obtaining information about products, applications such as 360° viewing of products and virtual trials have a significant impact on consumers' purchasing decisions (Markapoulos et al., 2006; Beck & Crié, 2016).

1.9 3.3. Risks of Digital Trade

- **Identity Theft**

This usually involves cybercriminals infiltrating e-commerce websites and stealing users' login or credit card details. Cybercriminals can then use users' identities to make fraudulent purchases or sell their personal information online to other criminals.

- **Fake Online Shops**

Unfortunately, not all e-commerce sites are trustworthy. Scammers can create fake websites to look like real sellers. By copying the design and layout and stealing logos, they trick users into believing they are on a trusted site. They attract attention by offering popular clothing brands, jewellery and electronics at low prices. Sometimes users pay for and receive the products they purchased. Other times, users do not receive their purchases at all.

- **Unencrypted Data**

Some websites do not encrypt data. Without an up-to-date and protected SSL certificate, they are more vulnerable to attack. Websites whose URL starts with HTTP instead of HTTPS are not secure; this poses a risk to shoppers who share credit card details and other sensitive information with these sites.

- **Data Breaches**

When you shop online, you share private data such as debit or credit card details, contact and address information with merchants. If hackers gain unauthorised access to an e-commerce website, there is a risk that this information could be exposed in the event of a data breach.

- **Fake Reviews**

Many online shoppers read reviews before purchasing a product. However, keep in mind that not all online reviews may be genuine. If there are reviews for a particular seller that seem too good to be true or lack enough detail, take care to check the source and trust your instincts.

- **Fake Apps**

Most of the real online sellers have specialised applications. However, cybercriminals may try to trick users by creating fake versions of these applications. Their aim is to obtain personal information such as bank or credit card details and usernames and passwords.

- **Unsecured Wi-Fi**

Unsecured Wi-Fi networks in public places can carry serious security risks. One of these risks is that hackers can position themselves between you and the connection point and monitor the data transfer. When you make online purchases over an unsecured Wi-Fi network, hackers can gain access to your personal data, such as credit card details and contact details.

- **Advertising Software**

Adware are unwanted adverts that appear on the screen when you browse the Internet. Adware is short for "adware" and is usually used to generate revenue for its owner. This software can be legitimate, but it can also be used maliciously by cyber criminals. For example, they can redirect you to malicious websites that try to get your personal

information. Sometimes, even clicking the "X" symbol to close a pop-up advert can cause problems.

- **Phishing Attacks**

This includes scammers who send fake emails that appear to be from a real seller. The emails often contain attachments or links designed to entice the recipient to click and, if clicked, can lead to malware infection (www.kaspersky.com.tr).

What kind of consumer am I?

This activity starts with the participants in a sitting position. Participants are given instructions to follow:

- If you shop a lot, stand up.
- If you shop in supermarkets, sit down.
- If you're ordering online, stand up.
- If you're selling online, sit down.
- If you find trading on the Internet easy, stand up.
- If you're attracted to the ad market, sit down.
- If you've been cheated on your online orders, stand up.
-

My Shopping Potential

Participants are divided into four groups. The groups are asked to choose one of the topics such as food, clothing, holiday, white goods, car etc. and design an advertisement poster for consumers in digital environment. Participants examine the

posters and choose the one that increases the desire to shop. The factors that increase the participants' desire to shop are discussed.

- What do you see on the poster?
- What does the poster say?
- Which detail in the poster is the most important for you? Why?
- Why are you thinking of shopping?
- What needs do you think this will fulfil after you've made this purchase?
- What's missing from the poster?
- What would you like to add to the poster?
- Do you like this image or not? Why do you like it?
- What emotions, feelings, memories does this poster evoke in you?

1.104. Digital Consumers

With the advancement of technology, mobile devices and increased use of the internet have transformed people's lifestyles and shopping habits (Ryan, 2016: 1660). These important and positive developments enable businesses to communicate with their target audiences through digital media and similar new channels. As consumers respond positively to these changes, the use of digital marketing has increased and this form of marketing has gained critical importance for businesses. Businesses are now faced with "digital consumers" and it is of great importance to understand the needs, habits and behaviours of this new generation of consumers. However, it should not be ignored that this process is full of difficulties (Alan, Kabadayı and Erişke, 2018:493).

E-consumers' reasons for shopping online:

- Quick Access
- Using from Home, Work
- Gaining prestige
- Comfort
- Being online

Points to be considered when shopping online

- Prefer sites with 3D secure system.
- Pay attention to seller security: Must use virtual POS
- Always check the SSL certificate.
- Shop with a virtual card.
- Set secure passwords.
- Beware of very cheap prices.
- Read the sales contract
- Always pay from your own computer.
- Check complaint sites
- Check the address and telephone number of the website (https://www.paynet.com.tr).

Acitivity:

Conscious Consumer

- Three different volunteer groups are formed from the participants.
- The animation process is shared among the volunteer participants by using situation cards.
- First group of situation cards: A young person asks his parents for support to upgrade his computer. The family gives the credit card details and password. The family reminds the young person to check the websites, pay attention to cheap prices, and check the address and telephone numbers of the websites. The young person shops by entering his family's credit card information on the computer of the workplace. A few days later, the young person receives a hair dryer instead of a computer and a lot of debts on his father's credit card... The following developments are dramatised by the group. The group is given a few minutes to prepare for the presentation. After the re-enactment, a conscious consumer directive is written together with the participants about what to pay attention to when shopping on the internet through digital tools.

- The second group is the status card: A man makes an online booking and pays for a holiday with his wife. The surprise of his wife makes her happy. When they go to the hotel for the holiday, they see that there is no such reservation and hotel... The following developments are animated by the group. After the reenactment of the second group, news about negative shopping experiences in the digital environment are researched, shared and discussed about the reasons.
- The third group is the status card: A woman constantly shops on the internet, whether she needs it or not, because it is easily accessible. The woman is an unconscious consumer, her husband suffers a lot from the situation and the economy of the house is in a difficult situation...The following developments are enacted by the group. After the role-playing of the third group, each participant measures his/her own carbon footprint by going to the website on being a conscious consumer.

Recommendations for Sustainability Consumers

Participants are divided into three groups; they choose one of the topics of food, clothing and goods and make a list of sustainable practices by researching on the internet and make a presentation to the group.

My Shopping ID

1. Who likes shopping?
   1. .....
   2.....
   3.....
   4.....
2. Face-to-face shoppers?
   1.....
   2.....
   3.....
   4.....

3. Internet shoppers?
   1 .....
   2.....
   3.....
   4.....
4. Shoppers who shop according to need?
   1.....
   2.....
   3.....
   4.....
5. Those who shop for non-essentials?
   1.....
   2.....
   3.....
   4.....

5 Those who pay attention to price
   1.....
   2.....
   3.....
   4.....

Participants are given "My Shopping Identity" papers and pens. Participants are asked to ask each other the questions on the "My Shopping Identity" papers in ten minutes and write down the answers given. The first one to write the names of four participants under each question wins the game. The participants form a circle and discuss the questions with the team (e.g: How people who shop according to their needs achieve this, why they shop online, etc.).

1.11What I learnt/found from the module

- What did you learn from this module, what did you find?
- The participants are instructed to write down what they have learnt and found on a notepaper.
- Participants are given a note paper and asked to write.
- The papers are hung on the board for everyone to see.
- The expectations written by the participants at the beginning of the module are compared with what the participants have learnt/found at the end of the module.

SOURCE

Abeliansky, A. L.,&Hilbert, M. (2017). Digitaltechnologyandinternationaltrade: Is it thequantity of subscriptionsorthequality of dataspeedthatmatters? *TelecommunicationsPolicy*(41), 35-48.

Akçi, Y. and Göv, S. A. (2015). ''Investigation of Consumers' E-Commerce Perceptions (Gaziantep and Adıyaman Sample)''.*Mehmet Akif Ersoy University Journal of Institute of Social Sciences, 7*(13), 412-415.

Alan, A. K., Kabadayı E. T. & Erişke, T. (2018). The New Face of Communication: Digital Marketing and Social Media Marketing, *Electronic Journal of Social Sciences, 17*(66).

Algharabat, Raed S. (2014). "Conceptualisingand modellingvirtualproductexperienceforonlineretailers". *International Journal of Internet Marketing andAdvertising, 8*(4): 300-319.

Algharabat, Raed, and Ali AbdallahAlalwan, Niripendra P. Rana, Yogesh K. Dwivedi (2017). "Three dimensionalproductpresentationqualityantecedentsandtheirconsequencesforonlineretailers: Themoderating role of virtualproductexperience". *Journal of Retailingand Consumer Services,* 36 (May): 203-217

Arslandere, M. (2010). *A Research on Electronic Commerce and SMEs in Karaman.* (Unpublished Master's Thesis), Karamanoğlu Mehmetbey University Institute of Social Sciences.

Artan, S. and Kalaycı, C. (2009). ''The Effects of the Internet on International Trade: The Case of OECD Countries''. *Journal of Doğuş University, 10* (2): 176-181.

Beck, Marie, and DominiqueCrié. (2016). "I virtuallytry it... I want it! Virtual FittingRoom: A tooltoincrease on-lineandoff-lineexploratorybehaviour, patronageandpurchaseintentions". *Journal of Retailing and Consumer Services*, 40(January):279- 286.

Bucaklı, A. T. (2007). *Electronic Commerce.* (Unpublished Master's Thesis), Istanbul: Kadir Has University Institute of Social Sciences, Department of Business Administration.

Civan, M. and BAL, V. (2002*). "E-Commerce and the Future of SMEs",* Kocaeli University Department of Economics and Business Administration, I. National Information, Economics and Management Congress / Proceedings Book, 10-11 May 2002 Hereke- Kocaeli.

Doğaner, M. (2007). *Electronic commerce in turkey' de electronic commerce development and a research on electronic commerce from business to consumer*, Selçuk University, Unpublished Master's Thesis, Institute of Social Sciences, Konya.

Elibol, H. and Kesici, B. (2004). ''Electronic commerce in terms of contemporary business management''. *Journal of Selçuk University Institute of Social Sciences,* 11, 304-329.

Kayahan, L. and Hepaktan, C. E. (2016). ''Var analysis on the factors affecting the volume of electronic commerce in Turkey''. *Ardahan University Journal of Faculty of Economics and Administrative Sciences*, 4: 159-190.

Küçükyılmazlar, A. (2006). *Electronic Commerce Guide.*Istanbul: Istanbul Chamber of Commerce Publications, Publication no: 2006-3.

Markopoulos, Panos M., and RaviAron, Lyle H. Ungar (2016). "Product information websites: aretheygoodforconsumers?". *Journal of Management Information Systems, 33*(3): 624-651.

Özdemir, F.B., Törenli, N. and Kıyan, Z. (2010). ''E-commerce model and regulatory regime-structure in terms of Turkey-European Union foreign trade relations''. *Ankara Journal of European Studies, 9* (2),117-143.

Özel, H. A. (2013). ''E-commerce and Turkey's Place in the Information Society''. *Journal of Academic Overview,* 38, 1-14.

Ryan, D. (2016).*Understandingdigitalmarketing: marketing strategiesforengagingthedigitalgeneration.* KoganPagePublishers.

Yeniçeri, T. (2008). ''Examining the factors affecting the tendency of SMEs to use electronic commerce with structural equation modelling''. *Erciyes University Journal of Faculty of Economics and Administrative Sciences*, 31, 145-163.

Yoo, Jungmin, and Minjeong Kim (2014). "The effects of online product presentation on consumerresponses: A mentalimageryperspective". *Journal of Business Research, 67*(11): 2464-2472.

MODULE 6

Digital Security

Module Scope

This module is a training programme that aims to provide trainers with knowledge and skills on digital security. Personal data security in the digital world, especially safe use in social networks, is one of the most critical issues faced by individuals and organisations. Educators' awareness of digital security is of great importance in transferring this information to students. This module covers personal data protection, security measures, social media usage and combating digital threats. Digital security has become even more important with the increase in digital threats encountered both in academic studies and in daily life.

Learning Outcomes

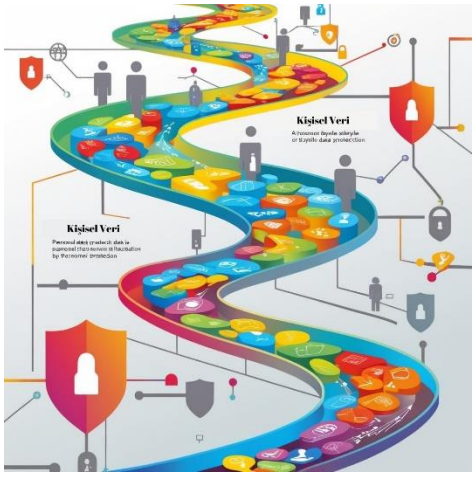
- To raise awareness about what personal data is and how it should be protected.
- To teach the methods by which personal data can be obtained and the measures to be taken to protect these data.
- To teach safe usage methods in social network applications.
- To ensure that individuals exhibit conscious and safe behaviours against the threats encountered in the digital world.

Content Tree

Digital Security

1. What is Personal Data?

Personal data refers to any information that can directly or indirectly identify an individual. In this context, information such as name-surname, Turkish ID number, e-mail address, IP address are considered personal data. Protection of personal data is one of the cornerstones of protecting individual privacy in the digital age. Studies on the protection of personal data emphasise the importance of controlling the data and obtaining approval before sharing it with third parties. Özkaya and Toprak (2022) examined the processing of personal data within the scope of security activities in Turkey. The researchers have analysed the legal dimension of personal data in depth. In the study, the problems experienced in the process of processing personal data and suggestions for solutions to these problems were presented. Awareness activities on personal data security should be increased. Various data breaches in Turkey and the introduction of KVKK (Personal Data Protection Law) have increased the awareness of individuals about the protection of their personal data. Data leaks, especially in the banking and telecoms sectors, have increased sensitivity on this issue.



1.1. I Track My Digital Footprint

1. Personal Data Scanning: Participants discover what information about themselves can be accessed in the digital environment by Googling their own names or usernames. Each teacher shares his/her findings with the group.

2. Group Work: Teachers are divided into groups of 3-4 people. Each group conducts research on a widely used social media platform (e.g. Facebook, Instagram, LinkedIn) and determines what personal data these platforms collect from users. They record their data on paper or on a digital note-taker.

3. Discussion and Conclusion: Discuss whether the information obtained as a result of both activities is secure or not, and how this information may pose a risk in terms of digital security.

Finally, the precautions to be taken regarding personal data sharing are discussed and the trainer guides the discussion.

2. Methods of Obtaining Personal Data

Personal data can be obtained through different methods in the digital world. Digital traces such as shopping on websites, social media posts, online surveys and the use of cookies can be collected by malicious people without authorisation. Fraud methods such as phishing and social engineering can also be used to make individuals unconsciously share personal information.

Non-digital methods are also used to obtain data. For example, personal information can be accessed through dumpster diving or physical seizure of mobile devices. Public Wi-Fi networks are also risky for stealing unencrypted data.

In the digital world, malware, spyware and keyloggers can be used to collect data from devices without authorisation. Social media platforms carry a great risk, especially in cases where security settings are weak, because personal information can be easily collected and used without authorisation. Altıntaş and Barkuş (2023)[1] , The security of our personal data is becoming more important day by day in this period where digital developments are and will continue to be experienced intensively. For this reason, it is of great importance to be aware of the threats to personal data security in digital environments and the measures taken to protect security.

2.1. Data Hunters

Scenario Based Game: Participants are divided into two groups:

Group 1: Assumes the role of "Data Hunters". They are tasked with collecting people's personal data through various online tools, such as a fictional social media platform or e-commerce site. For this purpose, they try to persuade users to share data by preparing permission request screens in applications, attractive campaign offers or online tests.

Group 2: As "Data Guardians", they try to pass the online scenarios created by group1 by sharing their personal information in a restricted way.

Evaluation and Feedback: After the activity is completed, both groups share their experiences. The data hunters explain which methods are more effective, while the data protectors share where they had difficulties and how they fell into data leakage traps. The trainer emphasises which data collection methods are common and which strategies can be used against them.

3. Measures to be taken in the Protection of Personal Data

Several basic measures can be taken to protect personal data:

- Use strong and unique passwords (e.g. €5k1$eH1r_BE instead of Eskişehir_83)
- Increase account security using two-factor authentication (2FA). To increase the security of an account, it enables authentication with an additional verification method, not just a password. For example, when logging into an email account, you first enter your password (the first factor). Then you are asked to enter a one-time verification code sent to your phone via an SMS or notification (second factor). This two-step process ensures that not only someone who knows the password, but also someone who has access to your phone can log into the account, making your account more secure.
- Beware of emails or files from unrecognised or insecure sources.
- To make regular software and operating system updates.
- Limiting the sharing of personal information on online platforms.

3.1. Cyber Security Simulation

Application

a. Participants are divided into small groups and each group is given a different scenario. The scenarios describe the situation of an individual or an organisation facing a data breach or a cyber-attack threat. For example:
   i. Group 1: Hacking of a social media account.
   ii. Group 2: Email phishing attack.
   iii. Group 3: Unauthorised data collection by an application.

b. Each group should identify the vulnerability in the scenario and discuss what measures they should take against this situation using the information provided and create a solution plan.

Presentation and Discussion: Each group presents their scenario and the solution plan they have developed to the other groups. The other participants give feedback on the solutions and the topic is discussed together. In this process, the trainer evaluates the accuracy of each solution and provides additional information.

---

4. Security in Social Network Applications

Social media platforms are areas where the majority of users share their personal information. If users unwittingly share too much information, malicious people may use this information to organise phishing attacks or security breaches such as account hijacking. Unauthorised transfer of shared personal information by platforms to third parties or advertisers may result in a violation of users' privacy. The following measures can be taken to avoid security vulnerabilities on these platforms:

- Sharing profile information only with people you know.
- Restrict who can access your information by adjusting security settings.
- Avoid clicking on suspicious links and pay attention to messages from unknown persons.
- Changing the passwords of social media accounts at regular intervals.

Ceyhan and Demiryürek (2015) examined how social media users in Turkey share their personal data and what kind of security measures they take during this sharing. The study revealed that most of the users do not pay attention to privacy settings. The hacking of the social media accounts of some celebrities in Turkey in recent years has highlighted the need to increase security measures on these platforms. "The Social Dilemma" documentary has attracted attention as an important production questioning the effects of social media on personal data security.

4.1. Creating a Secure Social Media Profile

30

Profile Analysis and Security Settings:

a. Participants choose one of the available social media accounts (e.g. Facebook, Instagram, Twitter).

b. Accompanied by the trainer, participants review and adjust the security settings of their chosen platform. They check which information is public and which information is visible only to their friends or themselves. The trainer draws attention to critical points in this process.

c. Additional security measures such as password strengthening, adding two-factor authentication, reviewing social media application permissions are demonstrated in practice to close security gaps for social media accounts.

Group Work Social Engineering Simulation:

a. Participants are divided into groups of 4-5 people. Each group works on a scenario based on social engineering. For example:
   i. A suspicious message from a friend's hacked account.
   ii. A phishing email or DM (direct message).

b. The groups determine which security measures should be taken against such attacks and formulate a solution strategy.

Presentation and Evaluation: Each group shares with the other groups the solution suggestions they have developed against the scenario they have encountered. The trainer evaluates these suggestions and makes suggestions for safer social media use.

2 APPENDICES

3 "Cyber Security Simulation" Event Scenario Examples

3.1 Group 1: Social Media Account Hijacking

A teacher's social media account was hacked and inappropriate content started to be shared from her account without authorisation. The account owner has realised this situation but cannot log in to his account. What steps should the teacher take to recover the account and avoid such a situation again?

3.2 Solution Proposals:

- Account recovery: The account holder recovers their account using the social media platform's account recovery tools (password reset or authentication).
- Activation of two-factor authentication (2FA): Use of an additional verification method when logging into the account (SMS, email verification or authentication apps).
- Use of strong passwords: Set a password that is more complex and difficult to guess, and avoid using the same password for different accounts.
- Monitoring suspicious activity: If any suspicious login or activity is noticed on the account, contact the social media platform or support immediately.
- Review security settings: Tighten account privacy and security settings and only log in from trusted devices.

3.3 Group 2: Email Phishing Attack

A teacher receives an email that appears to be sent by the school administration. The email contains a link to a system that needs to be updated. The teacher clicks on the link and enters his/her personal details (password, ID number). Shortly afterwards he realises that he cannot log in to his email account. What should the teacher do when he/she realises this attack and what precautions should he/she take to protect himself/herself from such attacks?

3.4 Solution Proposals:

- Change the password immediately: Anyone who realises they have been phished should immediately change their passwords (including email, social media, bank accounts, etc.).
- Using security software: Antivirus or anti-phishing software should be used to detect and clean the system of possible malware.
- Enabling two-factor authentication (2FA): Additional verification methods should be implemented to make accounts more secure.
- To check the authenticity of incoming e-mails: Before clicking on links in emails from places such as organisations or banks, check that the sender is official. Suspicious emails should be deleted or reported directly.
- Paying attention to personal information: Sensitive information (passwords, ID number) should never be shared via e-mail.

3.5 Group 3: Unauthorised Data Collection by the Application

A teacher uses a popular messaging app to communicate with his students. News about the app collecting user information without authorisation and selling it to third parties starts to spread. How

should the teacher evaluate this situation and what measures should he/she take to ensure the safety of his/her students?

3.6 Solution Proposals:

- Find alternative secure applications: Instead of apps that have been compromised or are known to collect personal data, alternative apps that are reliable and respect privacy should be preferred.
- Reviewing application permissions: Review what data the app accesses and limit permission to access personal data when it is not needed.
- Analysing the user agreement: Read the app's privacy policy in detail to find out what data is collected and share it with users.
- Utilising security software: Prevent malicious applications and data breaches by installing security software on mobile devices.
- To inform students and parents: To inform students and parents about data security and raise awareness about using safer digital tools.

4 "Creating a Safe Social Media Profile" Activity Scenario Examples

4.1 Scenario 1: Suspicious Message from Hacked Account

A teacher receives a strange message from a friend on his social media account. The message asks him to click on a link and share personal information. However, the message is not in the typical writing style of the friend and arouses suspicion. How should the teacher proceed in this case, considering that the account may have been compromised?

4.2 Solution Proposals:

Do not reply to the message and do not click on the link: Firstly, you should avoid responding to suspicious messages and clicking on links sent.

Contacting the friend through a different channel: The friend who is believed to be the owner of the account should use a different means of communication (phone, email) to verify whether the message is really from him/her.

Use of two-factor authentication (2FA): Teachers should enable two-factor authentication on their social media accounts and tighten security settings to prevent account compromise.

Changing the password and security checks: If the sender's account has been hacked, they should suggest that the friend change their password and go through the security checks of the social media platform.

4.3 Scenario 2: Phishing Email

A teacher receives an email purporting to be from her bank. The email contains a link stating that the teacher needs to update her account details. The link redirects to a fake website which looks very similar to the official website of the bank. The teacher suspects that this email may be fake and how should he/she strategise a solution?

4.4 Solution Proposals:

Verify the identity of the email: Examine the email address carefully and check whether it comes from an official source (e.g. find contact details on the bank's official website).

Not clicking on the link: It is important not to click on suspicious links and not to share sensitive information directly through such emails.

Contacting the bank directly: If the message is related to a bank, contact the bank's official telephone number or website directly to enquire about the authenticity of the e-mail.

Phishing reporting: The teacher should report such phishing emails to the relevant bank or platform and mark them as phishing to the email provider.

4.5 Scenario 3: Phishing Direct Message

A teacher receives a private message from a friend on a social media platform. The message states that the teacher has won a prize draw and asks her to share her personal details in order to claim the prize. The message contains a suspicious link and a request for a quick response. In this situation, the teacher is asked to determine what precautions he/she should take and what he/she should do to protect himself/herself from this attack.

4.6 Solution Proposals:

Analysing the message carefully: Analyse phishing indicators in the message, such as pressure to react quickly, promises of rewards and links.

Not clicking on the link: Instead of clicking on the link in the message, check the accuracy of the information through an official source.

Contacting the friend through a different channel: Contacting the friend through alternative means, such as by phone or another social media account, to check whether the message is really from the friend.

Increasing social media account security: Check security settings on social media accounts, activate two-factor authentication (2FA) and change passwords regularly.

Bibliography

1. Özkaya, E., & Toprak, B. (2022). Processing of Personal Data within the Scope of Security Activities in Turkey. *DergiPark*, 11(2), 79-95. https://dergipark.org.tr/en/download/article-file/2351149
2. Altıntaş, S., & Barkuş, F. (2023). A review on the concept of personal data security in digital environments. Electronic Journal of Vocational Schools, 13(2), 46-69. https://dergipark.
3. E. B. Ceyhan, E. Demiryürek, and B. Kandemir, "Current Security Risks and Protection Methods in Social Networks", UBGMD, vol. 1, sy. 1, pp. 1-10, 2015. https://dergipark.org.tr/tr/pub/ubgmd/issue/18272/192646
4. Kalkan, K., & Yılmaz, A. (2022). The role of digital security in education: A content analysis. *Journal of Education and Technology, 18*(3), 45-60.
5. Uzunoğlu, M. (2019). Digital security management in companies. *Journal of Cyber Security and Data Protection, 7*(2), 88-105.
6. Informatics Association of Turkey. (n.d.). *Digital security guide*. 20 October 2024, from https://www.tbd.org.tr
7. Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. New York: W.W. Norton & Company.
8. National Cyber Security Centre. (n.d.). *10 steps to cyber security*. Retrieved November 20, 2024, from https://www.ncsc.gov.uk

MODULE 7

Digital Ethics

Module Scope

This module aims to increase trainers' knowledge and awareness of ethical issues encountered in the digital world. Digital ethics is a concept that determines the responsibilities, rights and boundaries of individuals and organisations in digital environments. Ethical behaviour in the digital age covers important areas such as accuracy of information in online environments, personal data violations and digital property. It is critical for educators to exhibit conscious behaviours in these areas in order to provide students with the same awareness.

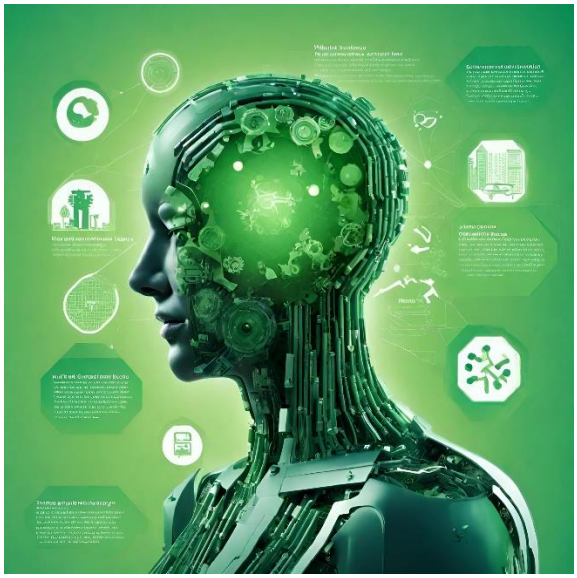
Learning Outcomes

- Defining the concept and importance of ethics in digital environment,
- Raising awareness on the protection of digital content and personal data,
- Recognise digital property and academic ethics violations and exhibit conscious attitudes towards them,
- Evaluating the limits and responsibilities of freedom of expression on digital platforms.

Content Tree

Digital Ethics

1. Concepts of Ethics and Morality
    - 1.1. Ethical Dilemmas Workshop
2. Breach of Personal Data
    - 2.1. Awareness with Critical Situation Cards
3. Accuracy of Information
    - 3.1. Race to Find the Right Information
4. Digital Property
    - 4.1. Rights and Responsibility Theatre
5. Academic Dishonesty
    - 5.1. Plagiarism Detective Study
6. Freedom of Expression
    - 6.1. Responsible Sharing Workshop



Digital Ethics

1. Concepts of Ethics and Morality

Ethics are the rules that determine the right and wrong behaviours of individuals in digital environments. Ethics are behaviours shaped in line with individuals' own value judgements. The importance of ethical rules in the digital world is increasing. Because anonymity in the online environment can cause individuals to cross boundaries.

1.1. Ethical Dilemmas Workshop

30

Case Presentation: Participants are presented with a short and thought-provoking case. For example, a teacher's unintentional breach of personal data when sharing student information or unethical behaviour on a social media platform.

Group Work: Participants are divided into groups of 4-5 people and each group discusses the case from an ethical point of view and develops solutions.

Result Sharing: Each group shares their solution suggestions with the whole class. The suggestions of other groups are evaluated and the ethically correct approach is discussed.

Conclusion and Feedback: At the end of the activity, the trainer makes a general evaluation of ethics and morality and gives feedback on how the participants can use these concepts more effectively.

2. Breach of Personal Data

Personal data protection is one of the most important ethical issues in the digital world. Although personal data violations are tried to be taken under control with the Personal Data Protection Law (KVKK) in Turkey, awareness on this issue should be increased. The amendments planned to be made within the scope of the Law on the Protection of Personal

Data should be realised without wasting time and especially the amendments to be made should be equivalent to the European Union regulations.

2.1. Awareness with Critical Situation Cards

Preparation and debriefing: When the participants enter the classroom, the trainer asks them to write down some of their personal data (e.g. name, surname, e-mail address) on a piece of paper/digital form.

Phishing Simulation: The instructor sends participants a fake email that appears to be a corporate email from https://www.proxynova.com/tools/send-anonymous-email/ "...". This email asks them to click on a link or download a file. Some participants may click on the link without realising this and unknowingly share their personal information on the fake page.

Identity Breach Surprise: During the activity, the trainer secretly creates fake social media profiles or emails in the names of certain participants and announces to the group that their digital identities have been stolen by saying "a compromise has occurred". At this point, participants see how easily fake identities can be created and how malicious people can manipulate this information.

Discuss the Consequences: The trainer will indicate to the participants the possible consequences of the breached credentials:

- Credit card fraud,
- Posts made from fake accounts on social media,
- Creating insecurity in work or social relationships,
- Fear and stress felt by people who experience vulnerability.

Solutions and Collective Discussion: Participants brainstorm what security measures they can take to prevent such breaches. Topics such as two-factor authentication, using strong passwords, email security, limited sharing of personal data are discussed.

3. Accuracy of Information

Distinguishing correct information in the digital environment is of vital importance, especially in the face of misinformation that has become widespread on social media and other information platforms.

3.1. Race to Find the Right Information

Distribution of Information Cards: Participants are divided into groups of 4-5 people and each group is given cards containing 5-6 news headlines. On these cards, some of the news items are real, while some of them are made up or consist of false information. Each group tries to determine which of the news given to them is real and which is fake by discussing. At this stage, they are allowed to check the source.

Discussion and Presentation: The groups present their findings and each group is asked to give a short explanation of how they determined the accuracy of the news. The trainer explains the accuracy or inaccuracy of each news item and the group discusses the reliability of the news sources.

Evaluation and Suggestions: The trainer gives feedback on the measures to be taken against fake information, how to recognise reliable sources and how to disseminate accurate information. In addition, participants are informed about fact-checking tools (Fact-Checking sites) in digital environments.

4. Digital Property

The protection of intellectual property rights in the digital environment is one of the most important ethical issues for content producers and users. Unauthorised sharing or use of digital content can lead to serious violations in terms of copyrights. In studies conducted in Turkey, it is stated that laws and awareness-raising activities for the protection of digital content should be increased

4.1. Rights and Responsibility Theatre

Case Studies: Participants are divided into small groups and each group is given a scenario related to digital property infringement. For example:

- **Group 1:** A teacher used an article from an online blog as a lesson material without permission.
- **Group 2:** A student shared a photo of another student on social media without permission from the owner.
- **Group 3:** Illegally downloading software and using it in a school.

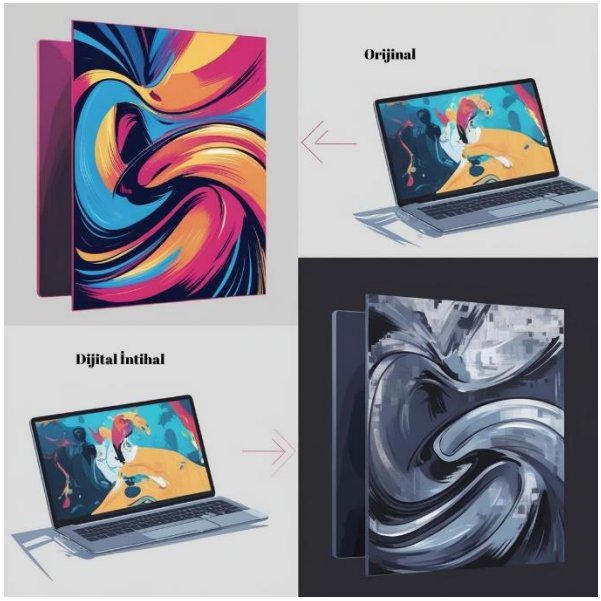
Each group analyses the property violation in its scenario, discusses why it is a violation and proposes solutions.

Presentation and Discussion: Groups present their scenarios and solutions to the other participants. Each group shares the information they have learnt about copyright, fair use and the use of licensed content by making a presentation. At this point, the instructor provides feedback to prevent misunderstandings.

Evaluation and Closing: Finally, the legal and ethical rules that should be considered in content production in order not to violate digital property are discussed. Participants gain awareness on how they can comply with the copyrights of the content they produce and share in the digital environment.

5. Academic Dishonesty

In the digital age, academic ethics has also undergone a major transformation. Especially as access to online resources has become easier, it has become more difficult to prevent ethical violations such as plagiarism. A study aiming to determine pre-service teachers' views on academic misconduct, their level of exhibiting behaviours involving academic misconduct and their reasons for doing these behaviours holistically revealed important results regarding the measures that can be taken for academic misconduct. In this context, it was determined that more than half of the pre-service teachers thought that academic misconduct was an unethical behaviour (59.2%), that practices to prevent it should be implemented (60.2%) and that they felt guilty when they exhibited such behaviour (53.5%). On the other hand, 50.3% of them stated that they had engaged in a behaviour that could be described as academic misconduct.



5.1. Plagiarism Detective Study

Case Study: "Academic Detectives": Participants are divided into groups and each group is given a case study. For example:

- **Group 1:** A teacher prepares a presentation using the article without citing the source.
- **Group 2:** A student presenting another student's research data as his/her own work.
- **Group 3:** A lecturer plagiarised a source from the internet and turned it into course material.
- The groups discuss whether there is academic misconduct by analysing the case example and propose solutions. Each group discusses what steps should be taken by considering ethical principles while proposing a solution.

Presentation and Discussion: The groups present their scenarios and proposed solutions to the other participants. The trainer provides additional information on the impact of academic misconduct on the quality of education and how to prevent such violations.

Evaluation and Closing: Each group receives feedback on what they need to pay attention to in order to uphold the principles of academic integrity. Participants develop a deeper understanding of academic integrity and learn how to follow ethical principles in the educational environment.

6. Freedom of Expression

While digital platforms expand freedom of expression, they also bring with them the responsibilities of this freedom. In the digital environment, individuals should use freedom of expression by respecting the rights of others.

6.1. Responsible Sharing Workshop

Debate Preparation: The participants are divided into two groups. Each group takes a position to organise a debate under the title "Freedom of expression should be

unlimited under all circumstances". One group argues that freedom of expression should be unlimited, while the other group argues that this freedom should be limited. The groups work on their arguments and plan how they will defend against the other group.

Debate: Each group presents its arguments in turn and the opposing group responds to the arguments. In this section, teachers are particularly encouraged to think about how they can create an environment of freedom of expression in their classrooms and how they can manage this freedom in an ethical framework.

Evaluation and Closing: After the debate is completed, a discussion is held with all participants. It is emphasised how freedom of expression should be handled in education and society, the difficulties that teachers may face in this regard and the solutions. The trainer makes suggestions on how to draw the boundaries of freedom of expression within an ethical framework.

Bibliography

Association of Information Technologies. (n.d.). *Digital ethics guide*. 3 November 2024, https://www.btd.org.tr

DataReportal. (2024). *Digital 2024: Global overview report*. Retrieved November 20, 2024, from https://datareportal.com/reports/digital-2024-global-overview-report

National Cyber Security Centre. (n.d.). *10 steps to cyber security*. Retrieved November 20, 2024, from https://www.ncsc.gov.uk

Özden, M., Özdemir Özden, D., & Biçer, B. (2015). *Mersin University Journal of Faculty of Education, 11*(2), 505-525. https://dergipark.org.tr/tr/download/article-file/161127

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. New York: W.W. Norton & Company.

Union of Turkish Bar Associations. (2022). *Digital Transformation and Law: The Effects of Digitalisation on Law*. Journal of the Union of Turkish Bar Associations, 2022(163), 2083. https://tbbdergisi.barobirlik.org.tr/m2022-163-2083.

Informatics Association of Turkey. (n.d.). *Digital security guide*. 20 October 2024, https://www.tbd.org.tr

MODULE 8

DIGITAL LAW

Module Scope

This module aims to enable teachers to gain competence in digital law. Digital literacy, digital health, digital access, digital communication, digital communication, digital commerce, digital security, digital ethics and digital rights and responsibilities constitute the Content Tree. Each title includes information and activities about legal situations encountered in the digital world. With this module, teachers develop awareness about the legal issues encountered in the digital environment and gain the ability to transfer these issues to their students correctly. The Content Tree aims to raise legal awareness and promote ethical behaviour in the digital world. The training aims to develop our awareness in accordance with the requirements of the digital age and to be an example to our environment and our students on these issues.

Learning Outcomes

Participants until the end of the module;

- Defines the concept of digital law.
- Explains the relationship between digital law and other dimensions of citizenship.
- Understands the legal framework by defining the components of digital literacy.
- Learns the legal problems encountered in digital health services and solutions to these problems.
- Emphasises the importance of digital access and legal regulations.
- Understands and applies ethical and legal regulations in digital communication.
- Learns legal regulations and practices in digital trade transactions.
- Understands digital security and legal framework.
- Understands the relationship between digital ethics and legal regulations.
- Understands the legal dimension of digital rights and responsibilities.

Content Tree

1. **Introduction**
2. **Digital Literacy**
    - Concept Map and Discussion
    - Key Words and Concepts
3. **Digital Health**
    - Case Analysis
    - Electronic Health Records and Privacy
4. **Digital Access**
    - Think-Pair-Share
    - Digital Access Challenges
5. **Digital Communication**
    - Pen Speaks
    - Ethics and Law in Digital Communication
6. **Digital Commerce**

- Socratic Dialogue
- E-Commerce Regulations

7. **Digital Security**
    - Brainstorming
    - Digital Security Threats
8. **Digital Ethics**
    - Values Chart
    - Digital Ethics
9. **Digital Rights and Responsibilities**
    - Group Discussion
    - Digital Rights and Responsibilities

1. Introduction

Digital law is a dynamic field that includes legal regulations in the context of internet and digital technologies. Both in Turkey and internationally, there are important regulations and laws in the field of digital law.

For example, in Turkey, the Personal Data Protection Law (KVKK) was enacted to ensure the protection of individuals' personal data (Personal Data Protection Authority, 2020). The PDPL introduces strict regulations on the processing, storage and transfer of personal data to third parties. This law is similar to the European Union General Data Protection Regulation (GDPR).

Internationally, the GDPR has contributed to raising digital data protection standards worldwide. GDPR aims to protect the personal data of individuals within the EU borders and imposes strict rules in this regard.

Intellectual property rights also have an important place in digital law. In Turkey, the Law on Intellectual and Artistic Works provides protection of creative works in the digital environment (Ateş, 2012). This law aims to prevent unauthorised copying and distribution of digital content. Internationally, the World Intellectual Property Organisation (WIPO) sets global standards for the protection of intellectual property rights.

Cybercrime is another important issue addressed under digital law. In Turkey, Articles 243 and 244 of the Turkish Penal Code regulate the fight against cybercrimes (Turkish Penal Code, 2020). At the international level, the United Nations has established various agreements and protocols on combating cybercrimes.

E-commerce regulations also have an important place in digital law. In Turkey, the Law on the Regulation of Electronic Commerce aims to ensure that e-commerce transactions are carried out in a safe and fair manner (Law on the Regulation of Electronic Commerce, 2014). Internationally, the OECD plays an important role in the regulation of e-commerce and the protection of consumer rights (OECD).

2. Relationship with Digital Literacy

Digital literacy includes the ability of individuals to search, use and produce information in digital environments. Knowledge of digital law enables the use of these skills within the framework of legal limits and responsibilities. Especially the management of privacy settings, protection of copyrights and legal content sharing are important components of digital literacy (Ateş, 2012). Digital literacy becomes more effective and secure when it includes digital law knowledge and skills. Therefore, understanding digital law is an integral part of digital literacy. Education programmes and awareness campaigns play an important role in increasing digital literacy (Bradford, 2020).

2.1. Concept Map

State your thoughts on the relationship between digital law and digital literacy in the form of a concept map. Discuss the concepts and the relationship with other participants.

Concepts

Digital Literacy: The ability to use digital technologies effectively and safely.
Data Protection: Ensuring the confidentiality of personal information.
Copyrights: Legal protection of digital content.
Online Security: Ensuring security on the Internet and digital environment.
Digital Ethics: Responsible and conscious behaviour in the digital world.
Information Access: Ability to access digital resources and information.
Media Literacy: Critical understanding of digital and traditional media.
Cyberbullying: Bullying and harassment in an online environment.
Digital Footprint: Personal data traces left on the Internet.
Online Identity: An individual's identity and personal information in the digital world.
Internet Ethics: Ethical rules to be followed while using the Internet.

Relationships

Digital Literacy & Data Protection: Digital literacy raises awareness of individuals about protecting their personal data.
Copyrights & Digital Ethics: Respecting the copyrights of digital content is part of digital ethics.
Online Safety & Information Access: Safe internet use increases access to accurate and reliable information.
Media Literacy & Digital Footprint: Media literacy ensures conscious media consumption by being aware of the digital footprint.
Cyberbullying & Online Identity: Online credentials must be protected against cyberbullying.
Internet Ethics & Online Safety: Adhering to Internet ethics improves online safety.

3. Relationship with Digital Health

Digital health involves the delivery of health services through digital technologies. Digital law provides for the protection of health information and records. In particular, electronic health records

and mobile health applications are subject to personal data protection and privacy regulations (European Union). In Turkey, the Personal Data Protection Law (KVKK) guarantees the secure storage and transmission of health information (Personal Data Protection Authority, 2020). The ethical use of digital health services and the protection of patients' rights are also regulated under digital law. These regulations ensure that digital health applications are safe and effective.

3.1. Case Analysis

More than one activity option is offered in the modules, the appropriate activity can be used.

Participants are divided into groups of four or five. Case scenarios prepared on the relationship between digital law and digital health are given to each group (Annex 1). Participants identify "Possible legal problems and solutions" in the scenario given by the group. (5') Groups share their scenarios with other participants. (5')

Case 1: Breach of Electronic Health Records

Scenario: A hospital experiences a data breach in its electronic health records system and patients' personal health information is accessed by unauthorised third parties.

Possible Legal Problems: Unauthorised sharing of personal data, breach of patient confidentiality.

Solution Suggestions: The hospital should implement emergency protocols in accordance with data protection laws such as KVKK and GDPR, inform the affected patients and take measures to increase data security.

Case 2: Data Collection of Health Apps

Scenario: A mobile health app collects users' health data without authorisation and uses it for commercial purposes.

Possible Legal Issues: Breach of privacy, breach of data protection laws.

Solution Suggestions: Application developers should collect user data in accordance with data protection laws and make data processing transparent. User approval processes should be strengthened.

Case 3: Cyber Attacks on Digital Health Systems

Scenario: A hospital suffers a cyber-attack and some of the patient information is compromised by ransomware.

Possible Legal Issues: Data security breach, cybercrimes.

Solution Suggestions: The hospital should implement emergency protocols, report the attack to the competent authorities and review cyber security measures to increase data security. Legally, more effective protection and sanction mechanisms against cyber-attacks should be developed.

Case 4: Wrong Treatment Due to Malpractice

Scenario: A hospital uses a digital application to track the treatment process of patients. However, due to an error in the application, some patients receive the wrong treatment.

Possible Legal Problems: Medical negligence, use of faulty software.

Solution Suggestions: Application developers and hospital management should perform regular checks and updates to increase the reliability and accuracy of the software. Rapid correction should be made and communication processes should be established to prevent harm to patients.

Case 5: Sharing Health Information with Employer

Scenario: A health insurance company assesses the health of job applicants by sharing the health information of its customers with employers.

Possible Legal Issues: Breach of confidentiality, unfair job evaluation.

Solution Suggestions: Health insurance companies should only share user data with user consent in accordance with the necessary confidentiality agreements. Unauthorised sharing of such information should be prohibited.

Case 6: Misleading Digital Health Ads

Scenario: A health product is promoted with misleading adverts on digital platforms and its health effects are exaggerated.

Possible Legal Issues: Misleading advertising, violation of consumer rights.

Solution Suggestions: Advertisers should promote the health effects of their products in an accurate and honest manner, and advertisements containing misleading information should be legally supervised and sanctions should be imposed.

Case 7: Breach of Confidentiality in Online Health Counselling

Scenario: An online health counselling service shares users' health information with third parties without their consent.

Possible Legal Issues: Personal data breach, privacy breach.

Solution Suggestions: Online health counselling services should process user information in accordance with data protection laws and take necessary security measures to prevent unauthorised sharing of this information.

Case 8: Misuse of Digital Health Data

Scenario: A research centre develops a commercial product using patients' digital health data without permission.

Possible Legal Issues: Personal data breach, ethical violations.

Solution Suggestions: Research centres should obtain data use permissions in an open and transparent manner and provide full information to data subjects about the purpose of data use. Ethical rules and data protection laws should be strictly followed.

4. Relation to Digital Access

Digital access refers to individuals' equal and fair access to information and services through digital platforms. Digital law plays a critical role in ensuring digital access. Legal arrangements are made to ensure access to digital platforms, especially for individuals with disabilities (Gökçen, 2018). In addition, states and international organisations develop various policies and programmes to eliminate digital inequalities and ensure that everyone can access digital resources (OECD). Digital law provides a basic structure for the protection and development of digital access rights. These regulations aim to make digital resources accessible to everyone.

4.1. Think-Pair-Share

Acitivity

Participants are asked what it means to be able to access information and services equally and fairly through digital platforms and what kind of problems especially disabled individuals may experience in this regard. For 1 minute, participants who think individually pair up with the participant next to them and share their thoughts with each other. (3') Volunteer participants are asked to share their thoughts on the subject with the whole group. (5')

5. Relationship with Digital Communication

Digital communication involves the transmission of information and messages through the internet and other digital platforms. Digital law ensures that this communication takes place within a legal framework. In particular, issues such as social media use, online harassment, hate speech and misinformation are addressed within the scope of digital law (Ersoy, 2021). Digital law sets privacy and data protection standards in digital communication and imposes legal sanctions in case these

standards are violated (Cini & Czulno, 2022). Thus, digital communication is ensured to take place in a safe and ethical manner.

5.1. Pen Speaks

Five pre-prepared flipcharts with the following topics are hung on the walls of the classroom (or corridor if not available). Participants are divided into five groups. Each participant is asked to take a pen in his/her hand. As the name of the activity suggests, participants are informed that only pencils will speak from this moment on. Each group is directed in front of a flipchart. Everyone is asked to individually write the problems and solutions that come to their minds about the concept they are in front of in one minute. At the end of one minute, the groups turn clockwise and individually write the problems and solutions for the next concept. After writing on all flipcharts, participants are invited to their seats. Five volunteer participants are asked to share what is written on the flipcharts with all participants.

Subject Headings

Hate Speech on Social Media

Online Harassment and Cyberbullying

Unauthorised Sharing of Personal Data

Infringement of Copyright

Digital Content Manipulation

Sample Problems and Solution Suggestions

Hate Speech in Social Media:

Issue: Spreading hate speech and misinformation on social media.

Solution: Legal regulations and platform audits should be increased, and user training should be provided.

Online Harassment and Cyberbullying:

Issue: Increasing incidents of harassment and bullying online.

Solution: Legal measures should be taken against online harassment and bullying, and victim support services should be strengthened.

Unauthorised Sharing of Personal Data:

Issue: Unauthorised sharing of personal data on digital platforms.

Solution: Comply with data protection laws, strengthen user privacy settings.

Infringement of Copyright:

Issue: Unauthorised copying and distribution of digital content.

Solution: Stricter enforcement of copyright laws, education and awareness campaigns.

Digital Content Manipulation:

Issue: Manipulation of digital content to spread misinformation.

Solution: Content verification mechanisms should be developed and sanctions should be imposed on those who spread false information.

6. Relation to Digital Trade

Digital commerce involves the sale and purchase of goods and services over digital platforms. Digital law ensures that digital commerce transactions take place in a safe and fair manner. E-commerce regulations cover issues such as the protection of consumer rights, the validity of electronic contracts and the security of digital payment systems (Law on the Regulation of Electronic Commerce, 2014). In addition, digital law aims to maintain fair competition on digital platforms and prevent unfair competition (Bradford, 2020). In this way, the healthy functioning of digital trade is ensured.

6.1. Socratic Dialogue

Socratic dialogue is a technique in which the subject is analysed in depth by asking questions and giving answers.

The trainer develops the critical thinking skills of the participants by asking the following questions to the participants and discusses the legal aspects of digital commerce with the participants.

Question 1: Why are consumer rights important in digital commerce?

Objective: To understand the importance of consumer rights protection in digital commerce.

Discussion: Participants discuss the consequences of violating consumer rights.

Violation of consumer rights can lead to a variety of serious consequences.
Financial Losses: The consumer may lose money because the goods or services purchased are incomplete or faulty. If returns are not accepted or compensation is not paid, the consumer suffers.

Trust Erosion: Consumers lose trust in digital platforms and e-commerce sites. This situation damages the reputation of the platforms and causes customer loss.
Legal Processes: Consumers may resort to legal remedies to seek their rights. This may lead to long and costly litigation processes.
Personal Information Security: Unauthorised use or sharing of consumer data is a personal data breach. This can expose the consumer to crimes such as identity theft and fraud.
Health and Safety: A consumer may face health and safety risks from a product or service that does not meet safety standards. This can lead to physical harm or serious health problems.

Question 2: How is Data Security Ensured in Digital Payment Systems?

Objective: To analyse the ways of ensuring data security in digital payment systems.

Discussion: Participants discuss the role of data protection regulations such as GDPR and KVKK.

GDPR (General Data Protection Regulation) and KVKK (Personal Data Protection Law) are legal regulations established to protect personal data and ensure confidentiality.
The GDPR applies throughout the European Union (EU) and aims to protect personal data in all EU member states. The GDPR requires data processing organisations to implement strict security measures and to grant data subjects various rights. For example, individuals have the right to access their data, to request deletion of their data and to be informed about how their data is used.
KVKK is in force in Turkey and aims to protect the personal data of individuals for similar purposes. KVKK obliges data processors to obtain the explicit consent of data subjects and to process personal data in accordance with the law and good faith.
These regulations aim to create a secure digital environment against data breaches by protecting the privacy of individuals. They also deter organisations that process data by providing for severe sanctions in the event of data breaches.
In short; GDPR and KVKK are the basic legal regulations that protect the rights of individuals in the digital world and ensure data security.
Data security in digital payment systems is ensured by various methods:
Encryption: Transmitted data is encrypted to protect the confidentiality of the data. In this way, the data is protected against unauthorised access.
Two-Factor Authentication (2FA): Adds an additional layer of security to users' accounts. Requires an additional verification method other than username and password to log in.
Secure Socket Layer (SSL) and Transport Layer Security (TLS): SSL/TLS certificates are used for secure payment transactions. This ensures that data is transmitted over a secure connection.
Tokenization: Sensitive data, such as credit card details, are exchanged for tokens that can be used only once. This ensures that security is maintained even if data is stolen.
PCI DSS Compliance: Compliance with payment card industry data security standards (PCI DSS) is an important step for data security. These standards set requirements for ensuring data security in payment transactions.
Up-to-date Security Software: Protect systems and data against malware by using antivirus and anti-malware software. It is also important that security patches are updated regularly.
These methods increase data security in digital payment systems, allowing users to pay securely and seamlessly.

Question 3: How to Protect Copyrights in E-Commerce?

Objective: To explore ways of protecting copyright in digital commerce.

Discussion: Participants discuss the unauthorised use of digital content and its legal consequences.

Legal Consequences:
Compensation Claims: If the copyright owner proves that he or she has suffered material damage due to the unauthorised use, the courts may award compensation.
Criminal Sanctions: In many countries, copyright infringement is considered a criminal offence and sanctions such as fines or imprisonment may be imposed.
Notice and Cancellation: Copyright holders may send a notice to remove the infringing content or cease its use. If the notice is not complied with, legal proceedings may be initiated.
Loss of Reputation: Organisations or individuals may lose their reputation and credibility due to copyright infringement.
Licence Fees: Copyright holders may charge licence fees to those who wish to use their content after unauthorised use.

Solution Proposals:
Licensing: To eliminate the risk of unauthorised use by obtaining legal licences before using digital content.
Credit: Respect the rights of original authors by giving proper credit to content owners.
Training and Awareness: Organising awareness-raising trainings on copyright and legal use of digital content.
Legal Consultancy: Professional counselling on legal processes and copyrights.
These legal measures and awareness-raising efforts help to prevent unauthorised use of digital content.

Question 4: What are the Legal Responsibilities between Seller and Buyer on Digital Platforms?

Objective: To examine the legal responsibilities of the parties on digital trading platforms.

Discussion: Participants discuss the responsibilities of the parties in terms of contract law and consumer rights.

Contract law and consumer rights provide a safe and fair trading environment by regulating the rights and responsibilities of the parties.

In terms of Contract Law
By Seller:
Delivery of Goods or Services: To deliver the goods or services specified in the contract on time and as defined.
Informing: Providing accurate and complete information about the product or service.
Warranty and Returns: To ensure that the product or service complies with the warranty period and return conditions.

By the Buyer:
Obligation to Pay: To pay the price specified in the contract at the time and in the manner specified.
Product Acceptance: To check and approve the delivered goods or services or to report defects.
Compliance with Contract Conditions: To act in accordance with other conditions specified in the contract.

In terms of Consumer Rights
Consumer Rights:
Right to be Informed: The right to have complete and accurate information about the product or service.
Right to Use Safe Products: The right to demand products or services that will not jeopardise health and safety.
Right of Return and Warranty: The right to have the product or service returned or repaired under warranty.
Right to Seek Rights: The right to resort to legal remedies in complaints and disputes.
Seller Obligations:
Open and Transparent Information: Providing consumers with transparent information about the product or service.
Providing Quality Service: To ensure the quality and safety of the product or service sold.
Compliance with Warranty and Return Conditions: To manage warranty and return processes by observing consumer rights.
Compliance with Legal Regulations: To act in accordance with consumer protection laws and regulations.
These responsibilities ensure that commercial relations between the consumer and the seller are carried out in a fair and reliable manner.

Question 5: What are the Legal Problems Encountered in the Logistics and Delivery Process and Solutions to These Problems?

Objective: To analyse the legal problems and solutions in the logistics and delivery process in digital commerce.

Discussion: Participants discuss the responsibilities of the parties in case of damaged or delayed deliveries.

Legal problems experienced in logistics and delivery processes in digital commerce are generally as follows:
Order and Delivery Problems: There are legal problems that may arise in terms of timely and correct delivery of orders. For example, delays along the supply chain or delivery failure.
Data Privacy and Security: Legal problems may arise regarding the protection and security of customer data. This includes situations where personal data may be accidentally shared or exposed to cyber-attacks.
Cargo and Logistics Services: It includes issues such as legal problems that may arise in contracts with cargo companies, uncertainty of cargo costs, cargo losses or cargo not being delivered on time.

Competition Law: Non-competitive behaviour in digital markets, such as price manipulation or copyright infringement, is also a legal issue.

The solutions are as follows:
Digital Transformation and Use of Technology: The use of technologies such as data analytics, artificial intelligence and blockchain makes logistics and delivery processes more efficient and secure.
Legal Regulations and Compliance: It is necessary to comply with the legal regulations of digital commerce, especially to be careful about data privacy and security issues.
Customer Communication and Support: Providing interactive and fast support services to improve customer satisfaction can be an important way to resolve issues quickly.
Competition Law Harmonisations: Digital markets should comply with competition rules and ensure that prices and services are offered in a fair and competitive manner.

The liability of the parties for damaged or delayed deliveries is generally determined by the sales contract and the applicable consumer protection laws.
By Seller:
Delivery Responsibility: The seller is obliged to deliver the product on time and undamaged. If the product is damaged or delivered late, the seller must ensure that the product is replaced or accepted for return.
Assurance: If the product is damaged during the delivery process, the seller assumes responsibility and must repair or replace the damaged product.
Information: It is the seller's responsibility to inform the customer about delays and potential problems in a timely manner.

By the Buyer:
Control and Notification: It is the buyer's responsibility to check the product immediately after receipt and notify the seller if there is any damage or deficiency.
Documentation: In case of damaged delivery, the buyer must provide the necessary documents (delivery receipt, damage report) and document the situation by photographing the product.
Logistics Company:
Damage and Loss Compensation: If the product is damaged during transport, the logistics company is obliged to compensate the damage.
Insurance: Transport insurance compensates the buyer or seller in the event of damage.
These responsibilities help to ensure a fair trade process by clarifying the rights and obligations of the parties.

7. Relation to Digital Security

Digital security refers to the protection of information and systems in the digital environment. Digital law plays an important role in ensuring digital security. Issues such as combating cybercrimes, protecting personal data and preventing data breaches are regulated under

digital law (Turkish Criminal Code, 2020). States and international organisations set cyber security standards and impose legal sanctions in case of violation of these standards (United Nations Office on Drugs and Crime). Thus, it is aimed to ensure security in digital environments and prevent cyber threats.

7.1. Brainstorming

Acitivity

Participants are divided into five groups. The groups are asked to create a list by identifying digital security threats. (3') The groups develop legal solutions for the threats on their lists. (3') The lists and solutions are shared with other groups. (3')

Common digital security threats are:
Identity Theft: By obtaining your personal information, they can open fake accounts or use your financial data.
Malicious Software: Malicious software such as viruses, trojans, spyware, etc. can damage your device or steal your information.
Cyber Attacks: Large-scale attacks can cause serious damage to governments, companies or individuals.
Data Leaks: Leaks of sensitive data could result in personal or organisational information being compromised.
Phishing Attacks: Attempts to capture your personal information using fake websites or emails.
Social Engineering: It tries to obtain personal information or confidential information by misleading people.
Human Error: Misbehaviour of employees with insufficient security awareness can threaten cyber security.
Security Vulnerabilities: Vulnerabilities of software or hardware allow attackers to gain access to their devices.
Ransomware: Locks your information or systems and demands payment.
Wi-Fi Threats: Advanced Wi-Fi threats may violate privacy.

Some effective solutions that can be taken against digital security threats are as follows:
Identity Theft:
Use strong and unique passwords.
Enable two-factor authentication.
Check your credentials regularly and report possible breaches.
Malicious Software:
Use antivirus and anti-malware software and keep it up to date.

Do not open email attachments and do not download files from unknown sources.
Update your software and operating systems regularly.
Cyber Attacks:
Use strong firewalls and network monitoring systems.
Get training in cyber security.
Back up your data regularly by developing backup strategies.
Data Leaks:
Use data encryption techniques.
Set strict access control policies and grant access only to necessary people.
Detect suspicious activity using data monitoring tools.
Phishing Attacks:
Be wary of suspicious emails and websites.
Organise Phishing awareness trainings and inform employees.
Use reliable email filtering software.
Social Engineering:
Train against social engineering attacks.
Authenticate before sharing sensitive information.
Use secure information sharing methods.
Human Error:
Clarify and tighten security policies.
Organise regular safety trainings.
Use technological solutions to minimise mistakes that employees may make unknowingly.
Vulnerabilities:
Update software and hardware regularly.
Perform security tests (penetration tests) to detect vulnerabilities.
If you use open source software, follow community updates.
Ransomware:
Regularly back up your important data and store these backups offline.
Avoid opening unknown email attachments and links.
Update your systems regularly and use security software.
Wi-Fi Threats:
Use strong and complex Wi-Fi passwords.
Prefer secure encryption protocols such as WPA3.
Use network monitoring software to monitor suspicious devices and activities.

8. Relation to Digital Ethics

Digital ethics deals with the ethical use of digital technologies and platforms. Digital law provides a legal framework for digital ethics. In particular, issues such as the ethical use of user data on digital platforms, transparency of artificial intelligence algorithms and ethical sharing of digital content are addressed within the scope of digital law (Güneş, 2019). Digital ethics and digital law aim to create a culture of responsible and conscious behaviour in the digital world. In this way, ethical and legal standards are protected on digital platforms (Kaya, 2021).

8.1. Values Chart

Participants create a list of digital ethical values. (2') Volunteer participants are asked to share the values they have identified. Legal implications of the identified values are discussed. (8')

Possible value and legal implications:
Confidentiality: To respect and protect the confidentiality of personal data.
Transparency: Being open and honest in information sharing and data processing processes.
Security: To ensure the protection of digital systems and data.
Fairness: Preventing discrimination and ensuring equality in digital services and algorithms.
Accuracy: Ensuring that information is accurate, complete and reliable.
Responsibility: The obligation to comply with ethical rules in the use of digital products and services.
Respect Respect the rights of users and their behaviour in the digital environment.
Privacy: Respect the privacy of individuals online and offline.
Consent: Obtaining users' explicit consent for the processing and sharing of data.
Accessibility: Ensuring that digital platforms are accessible to everyone.

The legal implications of digital ethics are protected and enforced through various laws and regulations:
Privacy The Personal Data Protection Law (KVKK) and the European Union General Data Protection Regulation (GDPR) protect the privacy of individuals' personal data and require data processing organisations to take strict security measures.
Transparency: The GDPR requires data processing organisations to be transparent in their data collection and processing. It ensures that users understand what data is collected and how it is used.
Security: Cybersecurity laws and regulations ensure that digital systems are protected and measures are taken against cyber attacks. These legal frameworks impose sanctions in the event of data breaches.

Justice Accessibility Laws ensure that digital services and content are accessible to everyone. They require that people with disabilities have equal opportunities in digital environments.
Accuracy: Misleading Advertising Laws require information published on digital platforms to be accurate and reliable. It imposes sanctions against misleading or false information.
Liability: Electronic Commerce Laws determine the responsibilities of providers of digital products and services. It includes regulations that protect customer rights.
Respect Online Harassment and Bullying Laws require respect for users' rights in digital environments. It imposes legal sanctions in cases of harassment and bullying.
Privacy Data Protection Laws ensure that individuals' online and offline privacy is protected. It includes legal sanctions against unauthorised data processing and sharing.
Consent GDPR and similar regulations require explicit and informed consent for the processing and sharing of data. It allows users to control their data.
Accessibility: Disability Rights Laws and WCAG (Web Content Accessibility Guidelines) standards ensure that digital platforms are accessible. Compliance with these standards is a legal requirement.

9. Relationship with Digital Rights and Responsibilities

Digital rights and responsibilities refer to the rights that individuals have in digital environments and the responsibilities arising from the use of these rights. Digital law provides a legal framework for the protection of digital rights and the determination of responsibilities (Doğan, 2021). In particular, issues such as the protection of personal data, property rights of digital content and freedom of expression online are regulated under digital law (Ersoy, 2021). Thus, it is ensured that individuals use their rights consciously and fulfil their responsibilities in the digital world.

9.1. Group Discussion

Acitivity

Participants are asked to identify problems and solution suggestions related to digital rights and responsibilities. (10') Group discussion is continued with volunteer participants.
Issues:
Privacy Violations: Unauthorised sharing and use of personal data.
Copyright Violations: Unauthorised copying and distribution of digital content.
Online Harassment and Bullying: Increased bullying, harassment and threats on digital platforms.
Data Security: Theft or leakage of sensitive information.
Disinformation: The dissemination of misinformation and fake news.

Access Barriers: Individuals with disabilities have difficulty in accessing digital platforms and content.
Inequality of Internet Access: Limited internet access in rural areas or low-income communities.
Cybercrime: Increase in crimes such as identity theft, fraud and malware.
Solution Proposals:
Privacy Breaches:
Strong data protection laws (e.g. GDPR and KVKK) should be implemented.
Companies and organisations should transparently determine and comply with their data privacy policies.
Copyright Infringements:
Copyright laws should be strictly enforced and sanctions for violations should be increased.
Digital platforms should use sophisticated monitoring and notification systems to provide protection to copyright holders.
Online Harassment and Bullying:
Stricter controls and policies should be implemented to prevent bullying and harassment on social media and digital platforms.
Users should be educated about online bullying and harassment.
Data Security:
Personal and sensitive data should be encrypted and secure data storage methods should be used.
Users and employees should be regularly trained on data security.
Disinformation:
Social media platforms should develop content verification systems to prevent the spread of fake news.
Users should be provided with media literacy training and taught how to identify the right information.
Access Barriers:
Digital platforms and content should be accessible for everyone. Special access solutions should be developed for people with disabilities.
Accessibility standards should be determined and these standards should be complied with.
Internet Access Inequality:
Internet infrastructure should be improved in rural areas and low-income communities.
State-sponsored programmes and projects should be initiated to close the digital divide.
Cybercrimes:
National and international cooperation should be increased to combat cybercrimes.
Awareness should be raised by providing training to users and institutions on cyber security.

Annex 1. Case Study Worksheet

Case 1: Breach of Electronic Health Records

Scenario: A hospital experiences a data breach in its electronic health records system and patients' personal health information is accessed by unauthorised third parties.

Possible Legal Issues:

Solution Proposals:

Case 2: Data Collection of Health Apps

Scenario: A mobile health app collects users' health data without authorisation and uses it for commercial purposes.

Possible Legal Issues:

Solution Proposals:

Case 3: Cyber Attacks on Digital Health Systems

Scenario: A hospital suffers a cyber-attack and some of the patient information is compromised by ransomware.

Possible Legal Issues:

Solution Proposals:

Case 4: Wrong Treatment Due to Malpractice

Scenario: A hospital uses a digital application to track the treatment process of patients. However, due to an error in the application, some patients receive the wrong treatment.

Possible Legal Issues:

Solution Proposals:

Case 5: Sharing Health Information with Employer

Scenario: A health insurance company assesses the health of job applicants by sharing the health information of its customers with employers.

Possible Legal Issues:

Solution Proposals:

Case 6: Misleading Digital Health Ads

Scenario: A health product is promoted with misleading adverts on digital platforms and its health effects are exaggerated.

Possible Legal Issues:

Solution Proposals:

Case 7: Breach of Confidentiality in Online Health Counselling

Scenario: An online health counselling service shares users' health information with third parties without their consent.

Possible Legal Issues:

Solution Proposals:

Case 8: Misuse of Digital Health Data

Scenario: A research centre develops a commercial product using patients' digital health data without permission.

Possible Legal Issues:

Solution Proposals:

Note: Each case scenario should be distributed to the groups by cutting from the places marked ---.

SOURCE

Ateş, M. (2012). Copyright in Intellectual Law. Ankara: Adalet Publications.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press.

Cini, M., & Czulno, P. (2022). Digital Single Market and the EU Competition Regime: An Explanation of Policy Change.

Doğan, C. (2021). Digital Rights and Responsibilities. Ankara: Seçkin Publishing.

Law on the Regulation of Electronic Commerce, 2014. Law No: 6563. Official Gazette No: 29166.

Ersoy, Ç. (2021). Digital Communication and Law. Ankara: Seçkin Publishing.

European Union. General Data Protection Regulation (GDPR). (Date of access: 28.10.2024).

https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules_en

Gökçen, Y. (2018). Digital Access and Equality. Istanbul: Beta Publications.

Güneş, Y. (2019). Digital Ethics and Law. Istanbul: Derin Publications.

https://copilot.microsoft.com/

Kaya, A. A. (2021). Artificial Intelligence Law. Seçkin Publishing.

Personal Data Protection Authority. (2020). Personal Data Protection Law. (Date of access: 28.10.2024).

https://www.kvkk.gov.tr/

OECD. E-commerce Regulation. (Access date: 28.10.2024).

https://www.oecd.org/sti/consumer/e-commerce.htm

Turkish Penal Code, 2020. Law No: 5237. Official Gazette No: 25611.

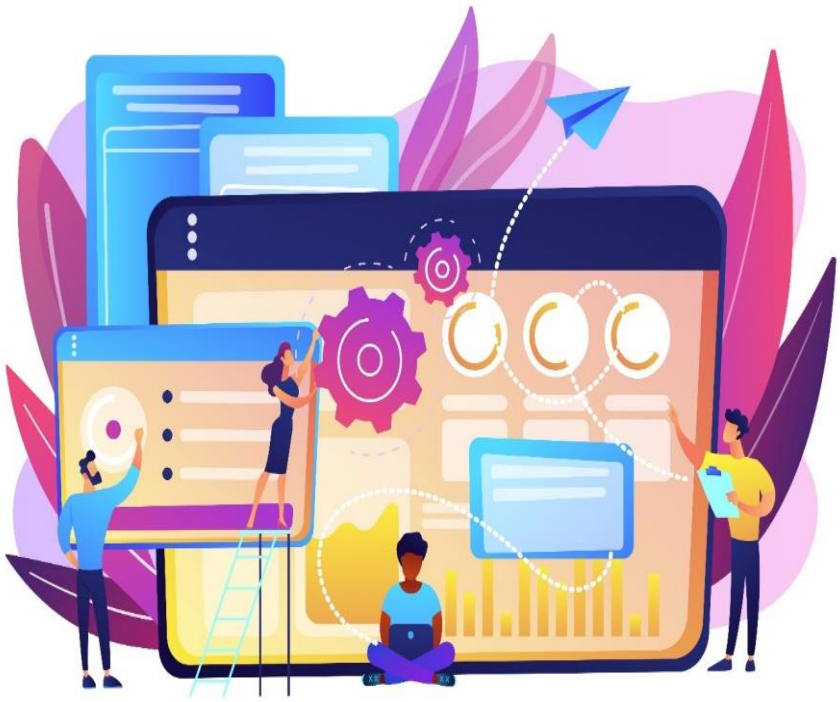
United Nations Office on Drugs and Crime. Cybercrime. (Date of access: 28.10.2024).

https://www.unodc.org/unodc/en/cybercrime/index.html

World Intellectual Property Organization. Intellectual Property. (Date of access: 28.10.2024).

MODULE 9

Digital Rights and Responsibilities



Module Scope

This module is a training programme that aims to enable trainers to gain awareness on "Digital Rights and Responsibilities" that gain importance with the concept of "Digital Citizenship" and to transfer this awareness to digital environments used in daily life and to their students. As citizens have rights and responsibilities in the traditional sense, digital citizens also have rights and responsibilities that they are obliged to fulfil in digital environments. It is important for digital citizens to be aware of and protect their own rights and responsibilities and to observe the rights and responsibilities of others (Council of Europe, 2019). In this context, digital rights and responsibilities will be discussed under five headings: the right to education, the right to protection of personal data, the right to access information and communication, the rights of individuals with special needs, and the rights of families and children.

Learning Outcomes

Participants until the end of the module;

- Will be able to define the rights and responsibilities of individuals in the digital society.
- Will gain awareness about the concept of the right to education and the equivalent of this right in the digital environment.
- Will gain awareness about the concept of the right to protection of personal data and the equivalent of this right in the digital environment.
- Will gain awareness about the concept of the right of access to information and communication and the equivalent of this right in the digital environment.
- Will gain awareness about the rights of individuals with special needs and the equivalent of these rights in the digital environment.
- Will gain awareness about the rights of family and children and the equivalent of these rights in the digital environment.

Content Tree

1. Introduction
    1.1. Discussion Rights and Responsibilities
2. Right to Education
    2.1. Right to Education in Digital Environment
    2.2. Group Work: How Teachers Evaluate the Right to Education in the Digital Transformation?

3. Right to Protection of Personal Data
    3.1. Right to Protection of Personal Data in Digital Environment
    3.2. Group Work: Personal Data Protection
4. Right of Access to Information and Communication
    4.1. Right to Access to Information and Communication in Digital Environment
    4.2. Discussion Circles: Access to Information and Communication
5. Rights of Individuals with Special Needs
    5.1. Rights for Individuals with Special Needs in the Digital Environment
    5.2. Think-Pair-Share: A Special Roadmap
6. Family and Children's Rights

    6.1. Rights of Family and Children in the Digital Environment

    6.2. Review: General Comment No.25 on the Rights of the Child in Digital Environments

Introduction

The development of digital technologies and making them available to society has enabled individuals to take an active part in digital environments. Digital right refers to individuals' access to information through technological devices in digital environments, the opportunity to create content and the freedom to publish the content they create (Bayzan, 2019), and the right to protect their personal information and privacy while doing so. The Turkish Language Association defines the word "responsibility" as "undertaking one's own behaviour or the consequences of any event that falls within one's jurisdiction". In this context, the individual's undertaking the consequences of his/her behaviours arising from his/her digital rights can be considered within the scope of digital responsibility. The fact that individuals are aware of their own rights and responsibilities and protect them also makes it necessary for them to be aware of and observe the rights and responsibilities of other individuals. In order to gain this awareness, it is inevitable that students should be given early education. Ribble (2011) stated that children should be educated about the concept of digital citizenship and the use of digital tools from an early age due to the gradual decrease in the age of using digital tools, and Selwyn and Facer (2007) emphasised the need for digital societies to provide support for children to make informed choices (cited in Yıldırım & Keser, 2022). Although there are measures taken by parents and institutions in the digital age, children's awareness of their rights and responsibilities will provide permanent solutions (Yıldırım & Keser, 2022). Therefore, educating and guiding children about digital rights and responsibilities is necessary in the context of digital citizenship. Students should be aware of their rights and responsibilities in digital environments (Elçi & Sarı, 2016; cited in Yılmaz, 2014).

The Turkish Century Education Model emphasises the importance of developing students' literacy skills. In the model, literacy skills are discussed under the subheadings of information literacy, digital literacy, financial literacy, visual literacy, cultural literacy, citizenship literacy, data literacy, sustainability literacy and art literacy. The process components of literacy skills in the Turkish Century Education Model are discussed at three levels. "These three levels are the level of awareness for defining, understanding, being aware of and showing sensitivity to the basic knowledge, terms, concepts and facts in the literacy type; the level of functionality for students to realise the holistic relationship between these knowledge, terms, concepts and facts; and the level of agency for students to act on the acquired knowledge. These levels are designed in a developmentally appropriate and spiral structure" (Ministry of National Education, 2024).

1.1.Discussion: Rights and

- **DISCUSS THE FOLLOWING QUESTIONS.**

✓ **WHAT RIGHTS AND RESPONSIBILITIES DO INDIVIDUALS/STUDENTS HAVE IN A DIGITAL SOCIETY?**

✓ **"HOW CAN INDIVIDUALS/STUDENTS GAIN THESE RIGHTS AND RESPONSIBILITIES IN A DIGITAL SOCIETY?"**

2. Right to Education

The right to education and human rights can be united under a common goal. Everyone should have the right to freedom, welfare and a life in accordance with human dignity (Akyeşilmen, 2014; cited in Binbir & Arastaman, 2021). The right to education is a fundamental right that enables people to use their potential in the most effective way by using their rights, freedoms and responsibilities. Thus, the individual contributes to both himself/herself and the society at a high level. Education is a process that primarily involves children through school and all age groups through different educational institutions (Güçlü, 2019; cited in Binbir & Arastaman, 2021). Ataman (2018) stated that the right to education is a fundamental human right and emphasised that everyone should benefit from education regardless of race, gender, ethnic origin, religion or political opinion, age, special educational needs (cited in Binbir & Arastaman, 2021).

2.1. Right to Education in Digital Environment

Digital technologies are rapidly gaining a place in the field of education. Especially after the COVID-19 pandemic, it can be said that this speed has increased and many individuals benefit from education in digital environment. As a natural consequence of digitalisation in daily life, the expectation of digital transformation in education is inevitable (Taşkıran, 2016; cited in Parlak, 2017). This transformation provides the diversification of digital tools, information and communication technologies used in educational environments. Some of the digital tools can be classified as "hardware", some as "software" and some as "environments" (Seferoğlu, 2014; cited in Parlak, 2017). The right to education in digital environments gains importance in this context. While digital transformation offers new opportunities, it is necessary to make certain arrangements to regulate the conditions, to ensure that every individual benefits from the right to education and to ensure equality of opportunity. Today, it is stated that increasing digital exclusion and digital illiteracy is a problem and effective ways to prevent it should be found (Siebert, 2010; cited in Parlak, 2017).

2.2. Group Work: How Teachers Evaluate the Right to Education in the Digital Transformation?

More than one activity option is offered in the modules, you can use the activity you find appropriate.

Discuss your thoughts on the right to education in traditional and digital environments in small groups of 3-5 people. Analyse the following questions in this context.

- What are the situations that violate the right to education in traditional and digital education environments?
- Considering traditional and digital education environments, what kind of situations have you encountered so far regarding the violation of the right to education?
- When comparing traditional and digital environments, in which environment is the violation of the right to education more visible?
- What are your suggestions for solutions to such violations of the right to education?
- If you were to sloganise your thoughts in support of the right to education, what would this slogan be?

3. Right to Protection of Personal Data

Human rights are recognised as inviolable and inalienable rights that individuals have from birth. Personal freedoms are rights that protect the individual against the state and society and are expressed as protective rights. Protection of personal data can be considered as a right arising from the fundamental right to privacy (Doğan, 2012). Personal data is defined as any information relating to a specific or identifiable person (Akgül, 2016).

> Personal data (Farina et al, 2008; cited in Akgül, 2016), which includes all information about a person, including not only his/her private life but also his/her economic and professional information, are data that reveal the identity of an individual, make a person specific and characterise him/her. A person's name, address, date of birth, marital status, nationality, profession, appearance, opinions (Şimşek, 2008; cited in Akgül, 2016), photograph, e-mail address, banking information, identity, pension, corporate registration and tax number, fingerprints, educational information, health data, phone messages, phone book, e-mail or writings, photographs, audio or video recordings written or shared on social networking sites such as Facebook and X are stated as personal data (Akgül, 2014; cited in Akgül, 2016).

The main purpose of the right to protection of personal data is to protect the individual through the protection of records kept by securing the privacy of the individual's private life (Claes et al, 2006; cited in Akgül, 2016).

In the KVKK Implementation Guide (2019), the purpose of regulating the Personal Data Protection Law (6698):

- To protect the fundamental rights and freedoms of individuals in the processing of personal data,
- To regulate (discipline) the obligations of natural and legal persons who process personal data and the procedures and principles to be followed,
- Protecting the privacy of individuals (right to privacy),
- It can be counted as ensuring personal data security.

3.1. Right to Protection of Personal Data in Digital Environment

The active use of digital technologies in daily life, health and education causes individuals to be involved in digital environments and to engage in behaviours. Individuals share their data in these environments. Protection of personal data is a necessity in digital environments that develop with the effect of digital transformation.

According to the statement made by UNICEF on 6 February 2018, around 175 thousand children access the internet for the first time every day, which means that a child accesses the internet every half a second. One out of every three internet users worldwide is a child. Along with the benefits and opportunities provided by digital access, risks and violations should also be taken into consideration. These risks can be listed as exposure of children to harmful content, cyberbullying and misuse of personal information. It is stated that the responsibility for protecting children in the digital environment lies with governments, families, schools and other institutions. Even when all these measures are taken, the most important protective method is for children to learn the rules in digital environments. They should be taught to protect themselves in digital environments, to be aware of their rights and to respect the personal space of others as well as to protect their own personal information. Children do not have the capacity to consent to the sharing, recording and processing of their personal data due to their age. In this context, children's presence in the digital environment leads to the sharing of their personal data, the storage of this information and the creation of profiles for this purpose. These profiles constitute a risk factor for the commercial use of third parties due to children's lack of digital literacy skills. In addition, the sharing of education and health data is also open to abuse (Esen Baygüneş, 2021). Another important issue is parental sharing in social media use. The concept of "sharenting" is a concept that refers to the sharing of information and images of the parent's child on social media. It creates a controversial situation when the parent crosses the boundaries of privacy and security without the consent of his/her child. This temporary "sharing" of the parent may cause situations that will negatively affect the adult life of the child in the long term (Esen Baygüneş, 2021).

3.2. Group Work: Personal Data Protection

Trainees are divided into two groups. Each group creates a checklist for the students to use. After the groups have created their checklists, they are asked to share the lists in the large group and talk about what the two checklists have in common.

- 1. The group prepares a list of measures that students can take to protect their personal data in their daily lives.
- 2.The group prepares a list of measures that students can take to protect their personal data in the digital environment.

4. Right of Access to Information and Communication

The Right to Information and Evaluation Authority (2021) defines the right to information as: "In the simplest sense, the right to information is the right of individuals to access the information that public institutions and organisations have due to their duties. It is stated that the right to information is regulated as an extension of the freedom of thought and expression, or it is seen as a separate right and added to the category of fundamental rights (Yalçınkaya, n.d.). With the right to information, information and information can be requested from organisations, and wishes and complaints can also be expressed (BEDK, 2021).

The right to communication is the right that enables people to improve their living spaces and express themselves everywhere. The right to communication can be considered from two perspectives: fundamental and inclusive. In the basic perspective, it is emphasised that everyone has the right to communicate. In the inclusive perspective, it is expressed as freedom of access to necessary resources and participation. In order to talk about the right to communication, communication resources must meet the basic needs of everyone (Şen & Şen, 2015).

4.1. Right to Access to Information and Communication in Digital Environment

As a result of the development and spread of the digital environment, access to information and the internet as a source of information can be mentioned. The increase in the variety of information presented and used in the digital environment (via the internet) can be considered both a result and a cause. It has become important to reach the information source with digital technologies without being dependent on access prevalence, low cost, interactive participation, time and place (Akkaya, 2017; cited in Akkaya 2021). The ubiquity of the internet shows that it is accessed as a source of information, the number of people who are regular internet users in the world has reached 4.66 billion as of the end of January 2021, and this group that accesses information includes people of all ages in terms of demographic characteristics (Akkaya, 2021).

It is stated that children have the right to access information, participation and communication in the digital age. The child's right to participation can be defined as expressing their own views on issues affecting their own and others' lives in the social and cultural sphere (Kaya, 2021). UNICEF on Children's Rights in the Digital Age; "In participation and the exercise of rights, children can benefit from the opportunities offered by digital media and develop resistance to the risks they face. As connected digital media users, children should be allowed to think critically, develop their own language, views, strategies, relationships and interests."

4.2. Discussion Circles: Access to Information and Communication

In groups of 10, form two discussion circles, one inner circle and one outer circle. Pair up with a participant in the circle and discuss the following questions Discuss.

- What can be done to ensure children's rights to access information, communication and participation?
- What are the risk factors for children's rights of access to information, communication and participation in digital environments?
- What can be done in educational environments to prevent these risk factors?

5. Rights of Individuals with Special Needs

Regulations are made in various laws to ensure the participation of individuals with special needs in society. United Nations Convention on these rights;

- ✓ That all human rights and fundamental freedoms (without discrimination) also apply to individuals with special needs,
- ✓ Equal opportunities, the need to be part of sustainable development strategies,
- ✓ Acceptance of the diversity within individuals with special needs,
- ✓ The need for all forms of support, empowerment and protection, control and rights to be treated with the same respect and attention everywhere in the world,
- ✓ Contributing to their full participation, development and lifting them out of poverty,
- ✓ Respect for their individual existence and independence,
- ✓ Protection against risks of neglect, abuse and ill-treatment,
- ✓ It emphasises rights and freedoms such as equal access to information, right to life, equality with others before the law, independent living, access to justice, freedom of thought and expression, access to education/health/rehabilitation, participation in cultural and social life (International Convention, 2009) and explains the concept of "having special needs" through interrelated rights and freedoms (Temiz & Yılmaz, 2021).

5.1. Rights of Individuals with Special Needs in the Digital Environment

In the digital age of digital transformation, individuals with special needs should have equal rights to keep up with this pace and benefit from the opportunities provided. Transformations in the field of special education vary according to the capacities of countries and institutions. Individuals with special needs have citizenship and human rights to access the same digital content at the same time and at the same cost as individuals without special needs (Lazar & Stein, 2017). Web accessibility is necessary for individuals with special needs to fully participate in the information age (Blanck, 2017). Digital accessibility is related to the ability of individuals with special needs to access electronic information resources such as websites, software, mobile devices and e-readers (Elder,

2017). Education is also important in terms of providing accessibility to digital technologies. The right to education, which is based on human rights, is extended to individuals with special needs through inclusive education. By integrating information technologies into primary and secondary schools, colleges and universities, lifelong learning and adult professional education environments, the accessibility of individuals with special needs to these educational opportunities is the key to sustaining inclusive education (Ziegler & Sloan, 2017). Although the social perception towards the use of communication technologies by individuals with special needs is low, the use of digital tools and the internet is actually promoted through many applications and projects (Köten & Erdoğan, 2014; cited in Oğuz Özgür, 2023). The issues addressed for individuals with special needs are generally determined as the problems experienced by individuals, accessibility, regulations in the field of education and health, and inclusion in working life (TOHAD, 2017; cited in Oğuz Özgür, 2023).

5.2. Think-Pair-Share: A Special Roadmap

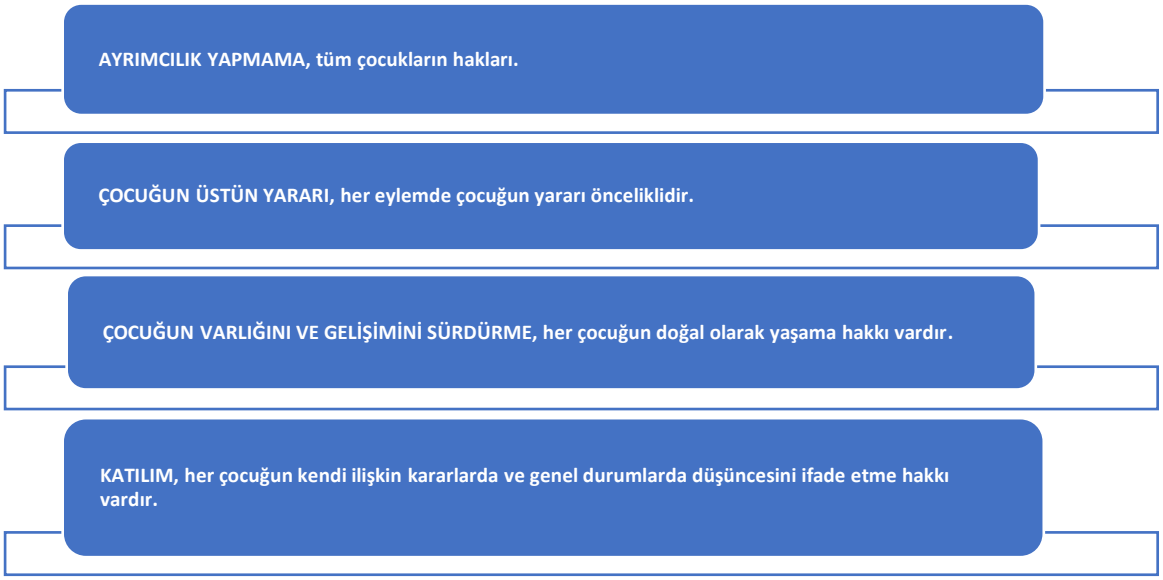
1. **Think (Individual-3'):** What can be done for individuals with special needs to keep up with the pace of digital transformation and realise their potential?
2. **Pair up (3-group work-7'):** Share your ideas with your group members. Which one(s) of these ideas can you implement in your classrooms? What would you need to implement them?
3. **Share (All participants-10'):** Share your discussion results with all participants. How can you transform the traditional classroom environment for individuals with special needs using these practices?

6. Family and Child Rights

The individual, who is the most basic building block of society, is both affected and influenced by the social environment in which he/she lives. The childhood years in which the individual develops are decisive on personality, values, attitudes and behaviours (Karatekin, 2016; cited in Kesayak & Karatekin, 2020). For this reason, physical, mental and spiritual development of the individual, being healthy and contributing to society can be realised by providing opportunities for this (Uçuş, 2013; cited in Kesayak & Karatekin, 2020). Children should have a family that respects children's rights in order to sustain their development (Gözütok, 2007; cited in Kesayak & Karatekin, 2020), but since families are not sufficient to protect children and meet their needs (Akyüz, 1983; cited in Kesayak & Karatekin, 2020), the necessity of granting special rights to children has emerged (Franklin, 1993; Kesayak & Karatekin, 2020). "Children's rights is the universal concept used to define all the rights that all children around the world have from birth, such as education, health,

life, shelter, protection against physical, psychological or sexual exploitation (Istanbul University Ç.K.U.M., n.d.)."

The four main principles of the Convention on the Rights of the Child express the basic requirements for the implementation of all rights. These principles are stated below (UNICEF; 1989);



When talking about the rights of the family, the concept of "Right to respect for family life" is taken into consideration. This right is regulated in Article 20 of the Constitution of the Republic of Turkey under the title of "Privacy of Private Life". According to this article, "Everyone has the right to demand respect for his private and family life. The confidentiality of private and family life shall be inviolable". Article 41, which is regulated under the title "Protection of the Family and Children's Rights", recognises that the family is the building block of society and obliges the state to take measures to ensure peace in family life, especially for the protection of mothers and children (Usta, 2022). Thus, while the family is responsible for the fulfilment of children's rights, the state is obliged to take measures to protect the rights of both the family and children.

6.1. Family and Child Rights in the Digital Environment

Social and environmental transformations affect both adults and children. In this age of accelerated digital transformation, the rights and responsibilities of children and adults are changing rapidly in this direction. The digital world transforms the social, economic, political and cultural structure with its impact on human life (Aral, 2022; cited in Sağlam, 2024) and changes the behaviour of children and the parenting styles of caregivers. Parenting is a belief system consisting of attitudes, perceptions, expectations, knowledge, values and action orientations towards the physical and social needs of children (Sağlam, 2024). "Mothers and fathers who can teach and guide their children to use technology correctly in the digital age period are called 'digital parents'." (Deniz, 2023). The parenting skills used to

minimise and mediate the negative effects of digital environments and technologies on children are called "parental mediation". The complexity created by digital transformation has left parents in a dilemma. On the one hand, they support the use of digital media for education and socialisation, on the other hand, they try to prevent the risks and negative effects (Sağlam, 2024). In this context, it is important for the parent to be both a "digital parent" and a "parental mediator" in order to ensure that children can exist in the digital environment in a healthy way by protecting their rights.

The United Nations Committee on the Rights of the Child published General Comment 25 on 24 March 2021 to explain the rights of children in the digital world. The rights of children in the digital environment specified in this document are shown as follows (UNICEF, 2024).

6.2. Review: General Comment No.25 on the Rights of the Child in Digital Environments

Read General Comment 25 of the United Nations Committee on the Rights of the Child **the Rights of Children in the Digital World**.

- In the context of the concept of "digital parent", how can you ensure that children exercise their rights and freedoms in the digital environment?
- What kind of practices can you do in your classrooms to transform the concept of "parent mediation" into "teacher mediation" for students in the digital world?
- What simultaneous measures in the family and educational environment can help children learn to both exercise and protect their rights in the digital world?

SOURCE

Akkaya, M.A. (2021). Internet perception as an information source and information access tool: a comparison of intergenerational approach differences. *Journal of Knowledge Management*, 4(2), 222-239

Bayzan, Ş. (2019, 6 November). What are our Digital Rights and Responsibilities. Retrieved on 17 October 2024 from https://www.guvenliweb.org.tr/haber-detay/dijital-hak-ve-sorumluluklarimiz-nelerdir

Information Acquisition and Evaluation Board (2021). 25 Questions on the right to information. Updated 2nd edition. Retrieved on 21 October 2024 from https://cdn.bartin.edu.tr/personel/5befd0afd1b74cd2936a909c89f8ccb9/287202113133525-soruda-bilgi-edinme-hakki.pdf.

Binbir, Ü. and Arastaman, G. (2021). The right to education: A systematic review study. *OPUS-International Journal of Social Research*, 18 (Special Issue on Educational Sciences), 5067-5098. DOI: 10.26466/opus.898503.

Blanck, P. (2017). Web Accessibility for People with Cognitive Disabilities: A Legal Right? In J. Lazar & M. A. Stein (Eds.), Disability, Human Rights, and Information Technology (pp. 41-57). University of Pennsylvania Press. http://www.jstor.org/stable/j.ctv2t4d02.7

Deniz, M.E. (2023, January). Digital Parenting. Retrieved on 22 October 2024 from https://tesam.org.tr/wp-content/uploads/2023/02/Mehmet-Engin-Deniz.pdf.

Elder, T. (2017). Open Government and Digital Accessibility. In J. Lazar & M. A. Stein (Eds.), Disability, Human Rights, and Information Technology (pp. 125-140). University of Pennsylvania Press. http://www.jstor.org/stable/j.ctv2t4d02.12

Esen Baygüneş, M. (2021, January). Protection of personal data of children in digital environment. *Journal of Başkent University Faculty of Law*, 7(1), 165-182. http://gcris.pau.edu.tr:8080/bitstream/11499/56582/1/NURULLAH%20YILMAZ.pdf

Istanbul University Child Protection Application and Research Centre. Child Rights. Retrieved on 22 October 2024 from https://cocukkoruma.istanbul.edu.tr/tr/content/cocuk-haklari-unicef/cocuk-haklari.

Kaya, L. (2021, 16 November). Participation, Expression, Access to Information: 3 Fundamental Rights of Children and Digital Media. Retrieved on 21 October 2024 from https://dijitalmedyavecocuk.bilgi.edu.tr/2021/11/16/katilim-ifade-bilgiye-erisim-cocuklarin-3-temel-hakki-ve-dijital-medya/

Kesayak, Y. and Karatekin, K. (2020) Investigation of Parents' Level of Implementation of Children's Rights in the Family. TÜBAD, 5(2), 313-335.

Kılınç, D. (2012). Protection of personal data as a constitutional right. *AÜHFD*, 61(3), 1089-1169

Development Process of Personal Data Protection Law. Retrieved on 18 October 2024 from https://nitelikliveri.com/kvkk-mevzuat/kisisel-verilerin-korunmasi-hukuku-gelisim-sureci/.

Law on the Protection of Personal Data (2016). Implementation Guide on the Law on the Protection of Personal Data. 6698, 24 March 2016

Lazar, J., & Stein, M. A. (2017). Introduction. In J. Lazar & M. A. Stein (Eds.), Disability, Human Rights, and Information Technology (pp. 1-8). University of Pennsylvania Press. http://www.jstor.org/stable/j.ctv2t4d02.4

Ministry of National Education, (2024). Turkey Century Education Model. https://tymm.meb.gov.tr/upload/brosur/2024programortakmetinOnayli.pdf

Oğuz Özgür, H. (2023). Current threat area of disabled individuals: The online world. *Barrier-Free Informatics 2023: Barrier-Free Digital Transformation*. 27-47

Parlak, B. (2017). Education in the digital age: an analysis on possibilities and applications. *Journal of Süleyman Demirel University Faculty of Economics and Administrative Sciences*, 22 (Kayfor15 Special Issue), 1741-1759.

Sağlam, T. (2024). Technology use and digital parenting in children. *Journal of Individual and Society Social Sciences*, 14(1), 123-129. https://doi.org/10.20493/birtop.1496639

Sağlam, T. (2024). Technology Use and Digital Parenting in Children. *Journal of Individual and Society Social Sciences,* 14(1), 123-129. DOI: 10.20493/birtop.1496639

Şen, A. F., & Şen, Y. F. (2015). An evaluation on social media, right to communication and freedom of expression. *Gazi University Journal of Faculty of Economics and Administrative Sciences*, 17(2), 122-136.

Temiz, N. Ve Yılmaz, B. (2021) Investigation of educational policies for students with special needs in primary and secondary education in Turkey. *Yaşadıkça Education*, 35(1), 104-131.

Türk Dil Kurumu (n.d.) Türk Dil Kurumu Dictionaries. Retrieved on 17 October 2024 from https://sozluk.gov.tr/.

UNICEF (2024). General comment no.25 on children's rights in digital environments. Retrieved from https://www.unicef.org/turkiye/media/17626/file/Dijital%20Ortamlarda%20%C3%87ocuk%20Haklar%C4%B1%20ile%20%C4%B0lgili%20Genel%20Yorum%20No:%2025.pdf on 22 October 2024.

UNICEF Turkey National Committee, (1989). About the Rights of the Child. Retrieved on 22 October 2024 from https://www.unicefturk.org/yazi/cocuklar-icin-bilgi.

UNICEF, (n.d.). Children's Rights in the Digital Age. Retrieved on 21 October 2024 from https://www.unicef.org/turkiye/media/2606/file/TURmedia_Dijital%20Cagda%20Cocuk%20Haklari.pdf%20.pdf.

UNICEF Turkey National Committee. The obligation to protect children in the digital world. Accessed on 21 October 2024 from https://www.unicefturk.org/yazi/-internetgunu?gad_source=1&gclid=CjwKCAjw1NK4BhAwEiwAVUHPUPaDZckyD8taMhaOjs_-ZLWBlEUEyi23aswMzZS6EcZcp7gsqZ5HVhoCbHYQAvD_BwE.

Usta Ö. (2022). Respect for Family Life and Examination on Several Institutions Handled in the Context of the Right to Protection of Family Life. *SUHFD*, 30(3), 1561-1590.

Yalçınkaya, B. (n.d.) Access to information and sustainable development. *UNESCO Memory of the World Programme.* 21 October 2024 at https://www.unesco.org.tr/Content_Files/Content/buyukbulusmalar/3bb/i5.pdf

Yıldırım, S., & Keser, H. (2022). Digital rights and responsibilities scale development study. *Pamukkale University Faculty of Education Journal (PAUEFD)*, 61, 414-437.

Yılmaz, N. (2014). *The relationship between digital citizenship perception levels and information literacy perception levels of administrators and classroom teachers.* [Master's Project without Thesis, Pamukkale University]. Pamukkale University Open Access System.

Ziegler, M. J., & Sloan, D. (2017). Accessibility and Online Learning. In J. Lazar & M. A. Stein (Eds.), Disability, Human Rights, and Information Technology (pp. 158-181). University of Pennsylvania Press. http://www.jstor.org/stable/j.ctv2t4d02.14

MODULE 10

Adult Education and Local Trainings

Learning Outcomes

- Will have knowledge about the contribution of in-service trainings to the professional development of teachers.
- Will have knowledge about the learning processes of adults.
- Realise the importance of communication skills.
- Will have knowledge about new approaches in professional development of teachers.
- Recognise the steps to be followed in local teacher trainings.

1. Introduction

The concept of lifelong learning is gaining more and more importance today. It has become an important necessity to continuously support their professional and individual development and to ensure that they keep up with current developments.

School administrators and teachers are the ones who bring educational policies, reforms, curricula, technological developments together with students in an education system and carry these innovations into practice. In-service training activities allow educators to update and expand their professional skills. These trainings allow staff to learn new techniques and methods while increasing their knowledge.

For qualified teachers and qualified teaching, it is necessary to provide continuous support to teachers and school administrators for professional development. In this respect, in-service training activities are organised for the professional development of teachers and school administrators, personal and professional development programmes are developed with the support of experts and institutions and implemented within the scope of in-service training.

Within the scope of professional development of teachers, informing them about new approaches, methods and techniques used in education and training, increasing their professional knowledge and skills, and improving their skills in the use of new technologies and technological environments were prioritised.

In-service training activities are planned and carried out in line with the professional development areas identified by teacher needs analyses, as well as the policies and priorities of the Ministry of National Education and the areas indicated by the top policy documents.

2. New Approaches in Professional Development of Teachers

Today, new approaches are applied in different countries of the world to ensure the professional development of teachers. In this context, while in-service training activities in our country are organised as courses and seminars in line with standard training programmes, they have started to be carried out in the form of "teacher-administrator mobility programmes", "school-based professional development (SBPD) programmes", professional development communities (PDC) within the scope of "Ministry of National Education Personnel In-Service Training Regulation[2] " which entered into force on 11 March 2022. These new approaches are put into service in the Teacher Informatics Network (TIN) established to support the professional development of teachers.

2.1. School Based Professional Development (SBPD): In-service training activities organised within the scope of the local in-service training plan in order to meet the training needs identified by the school and specific to that school.

2.2. Professional Development Communities (PDC): Professional Development Communities (PDT) are organised to improve education and training practices at school, to increase the professional knowledge and skills of the participants, and to ensure their professional development by learning from each other and from practice. The intra-community communication of the Professional Development Communities and the sharing of the work done are carried out through ÖBA.

2.3. Teacher-Administrator Mobility Programme: This programme is organised to share the knowledge and experience of schools that stand out with their success, good practices, different projects or different learning environments and to enable teachers and administrators working in other schools to visit these schools.

3. Considerations in Adult Education

It is important to create meaningful learning experiences appropriate to the age and interests of adults. It will be more effective to provide practical and applicable information instead of theoretical information. Using examples that offer solutions to situations and problems encountered especially in business life makes the learning process more efficient. Adults do not like to be passive recipients. Active participation should be ensured through games, team work and problem solving exercises. A large part of learning takes place with visual elements. Presenting information in an aesthetically and visually interesting way increases retention. Asking questions that will allow them to produce solutions keeps interest alive and encourages thinking.

Communication Skills

Effective communication skills in adult education are very important to make the education process effective and efficient. Particular attention should be paid to active listening, empathising, clear and clear expression, giving feedback and use of body language during the training.

Acitivity

You can apply the activity given below with the participants to understand the importance of communication skills.

Signalling Game: In order to draw attention to the problems we experience while communicating, it is a game in which the participants try to transmit the signal given by the person leading the game as a group to their friends at the head of the group in the fastest way. Before starting the game;

1) Divide the participants in the class into two groups (maximum of fifteen).
2) Ensure that each group sits in a straight line with the help of chairs.
3) Place an item such as a bottle etc. one metre in front of the two front chairs at an equal distance for the participants to get up and pick it up when the signal is given.
4) Ask all participants to put a hand on the shoulder of the participant in front of them.
5) Sitting among the participants at the back of the room, toss a coin in the air and indicate to the player in front that, depending on whether the coin lands heads or tails, the players should squeeze the shoulder of the player in front if the coin lands tails, but should do nothing if it lands heads.
6) Each player has to squeeze the shoulder of the player in front of him and deliver it to the first player as quickly as possible.
7) The players at the front will try to grab the object in front of them when they receive the signal. The first group to take it will be able to move forward one row. The game will be completed when the player who started first comes back to the front row.

After the game, you can summarise all the factors that can be experienced in the "communication process" by asking the participants to share the difficulties and misunderstandings they have experienced.

Communication Tools in Adult Education

In adult education, traditional educational tools are used as well as a variety of digital communication tools suited to the needs and interests of adult learners. These tools play an important role in helping adults to develop their knowledge and skills.

Acitivity

Conduct a brainstorming session to get participants' views on digital tools that can be used in adult education and how to use them. Do not forget to do this brainstorming on a digital tool.

4. Local Teacher Trainings

Local teacher trainings are planned together with the branch managers responsible for in-service trainings in provincial national education directorates. Our teachers who have received the training of trainers are expected to participate in the planning process together with the branch managers in their provinces and provide Digital Citizenship trainings in their provinces.

During Training

After the training plans are made, the trainers are expected to provide training in accordance with the professional development programme of the course with the determined dates and participants. In addition to these modules prepared for the course to guide the trainers, you can also direct the participants to complete the "Digital Citizenship Education" course on Teacher Information Network (TIC) before coming to the training. This will help participants to complete the theoretical knowledge online. You can access the professional development programme of the course from the "Courses" folder on the website of the General Directorate of Teacher Training.