

STANID

SUPPORTING CONTINUED ACCESS
TO EDUCATION ENHANCING
SCHOOLS' DIGITAL READINESS



PR3 - Handbook:
Data protection and
safety in distance



Co-funded by
the European Union



SZKOŁA PODSTAWOWA
im. św. Jana Kantego
w Białymostku



ΑΡΙΣΤΟΤΕΛΕΙΟ ΚΟΛΛΑΓΙΟ



Authors



**DANMAR
COMPUTERS SP
ZOO**

www.danmar-computers.com.pl

ΑΡΙΣΤΟΤΕΛΙΟ ΚΟΛΛΕΓΙΟ

**ARISTOTELIO
COLLEGE**

www.aristotelio.edu.gr



**Szkola
Podstawowa im.
sw. Jana
Kantego w
Będziemyslu**

<https://bedziemy.sl.szkolna.net/>



**STIMMULI FOR
SOCIAL
CHANGE**

www.stimmuli.eu



**CENTRO PER LO
SVILUPPO
CREATIVO
DANILO DOLCI**

www.danilodolci.org



**BLUE ROOM
INNOVATION SL**

www.blueroominnovation.com



Escola la Bòbila

<https://agora.xtec.cat/escolabobila/lescola/>



ISTITUTO COMPRENSIVO
CASSARA-GUIDA

**I.C. Cassarà-
Guida**

www.istitutocomprensivocassara.gov.it

Table of Contents

STAND Project	6
Activities and Results	6
Introduction to the STAND Handbook.....	7
Target Group.....	9
Learning Objectives for parents and teachers.....	9
Learning Objectives for students	10
Chapter 1- Critical processing of digital information.....	11
Fake news.....	11
Identifying fake news and clickbaits	15
Chapter 2 - General notions on data protection policies	20
Introduction to GDPR and national laws	20
GDPR terms and definitions.....	21
GDPR obligations for processing personal data	24
GDPR user rights	25
Chapter 3- Digital Threats and Cybersecurity.....	27

Cybersecurity in the education sector and common digital threats	27
Cybersecurity Measures and Technologies	33
Chapter 4- Digital Identity.....	36
Definition of Digital Identity	37
How Digital Identity affects our social and daily life	37
How to protect our Digital Identity.....	39
School and Digital Identity: good practices	40
Chapter 5- Online behavior – rules, risks, and advice	42
Online behaviors, risks, and legal consequences	43
Negative consequences on development and well-being.....	47
Using the internet responsibly: tips for parents, teachers, and children.....	48
Conclusions	54
Classroom Activities	55
Lesson Plan 1- Sherlock Holmes of Fake news	56
Lesson Plan 2- Privacy and GDPR.....	58
Lesson Plan 3 - Be suspicious.....	59

Lesson Plan 4- Cyber threats awareness	61
Lesson Plan 5- Myself on social media	63
Lesson Plan 6 - Let's build together a better internet!.....	65
Annex	67
References	79
Agencia Española de Protección de Datos, Autoritat Catalana de Protecció de Dades, Agencia Vasca de References	79

STAND Project

STAND- SupportTing continued Access to education enhancing schools' Digital readiness is a two-year European project funded by Erasmus+ Programme, under KA2 Cooperation Partnerships in the field of school education. It started in 2021, facing the ongoing difficulties caused by the global pandemic of COVID-19.

The aim of the STAND project is to equip teachers and educational staff, as well as students and their families, with the necessary skills, tools, and personalized support to address the challenges of the digital age to ensure the full and equal participation of all students in education.

The STAND project has already provided ICT and digital support to teachers, parents, and students, while introducing fresh training opportunities to equip teachers and staff in primary and lower secondary schools with the necessary digital competencies for effective digital learning and teaching.

Activities and Results

Massive Open Online Course (MOOC)

A free online course has been developed and it is available for anyone to enroll, addressed to teachers for developing and reinforcing their digital skills

In September 2022, the trainers from partner organisations met in Poland to prepare themselves for the delivery of the STAND course.

During the scholar year 2022/2023, more than 150 teachers have participated to the piloting of the STAND MOOC

Methodological Guide

Together with participating schools, the partners have developed a methodological guide with strategies and principles for effective digital education. The content of this guide is delivered to teachers through workshops on digital integrated pedagogical methodology through practical and nonformal activities.

Data protection and safety in distance learning Handbook

STAND Handbook- the document you are reading right now- offers additional resources about data protection and safety in digital learning for teachers, parents and students. The content of this Handbook will be delivered through 6 info-sessions in each country that will be organized to raise awareness about a responsible use of the digital tools, online safety and data protection.

STAND Alliance platform

The STAND Platform will remain available as a free space for teachers and parents for peer-support, interaction and peer-learning. A final conference in Spain and final events in Italy, Greece and Poland will take place at the end of the 2023 for presenting the final project's results and outcomes.

All results and further information are available in the project's website <https://standproject.eu/> in 5 languages (English, Italian, Greek, Polish and Spanish).

Introduction to the STAND Handbook

The “Data protection and safety in distance learning” STAND Handbook is both theoretical and practical. It provides teachers and parents with theoretical input on different aspects of safety in online learning, while it also includes activities for classroom implementation to raise awareness

among primary and secondary school students on the dangers they may encounter when they are online and on the importance of protecting their data and digital identity. The “Data protection and safety in distance learning” STAND Handbook consists of the following 8 sections:

- **Introduction-** It introduces readers to the “Data protection and safety in distance learning” STAND Handbook, including the target group and learning objectives for teachers, parents, and students.
- **Chapter 1 - Critical processing of digital information.** It aims to provide guidelines and tips on recognizing and avoiding fake news and finding reliable sources of information online.
- **Chapter 2 - General notions on data protection policies.** It covers the main aspects of the GDPR, including definition of key concepts related to personal data.
- **Chapter 3 - Digital threats and cybersecurity.** It presents the threats that may occur when using ICT systems and the measures that need to be taken at school level.
- **Chapter 4 - Digital Identity.** It provides guidelines on digital identity, including the definition of digital identity, and the measures we can take to protect our digital identity.
- **Chapter 5 - Online behavior – rules, risks, and advice.** It explains how to support children in using the internet consciously and presents the most prominent risk phenomena that can be harmful to their health and well-being.
- **Classroom Activities-** It includes 6 lesson plans ready for classroom implementation targeted to primary and secondary school pupils. The lesson plans include the description of the activities, target audience, age, time needed for preparation and implementation, learning

outcomes, resources (both online and offline) and a detailed description of all steps for its implementation at school. The lesson plans are related with data protection, online safety, and digital threats.

- **Annex-** It contains the worksheets to be used when implementing the lesson plans found in the Classroom Activities section.

Target Group

The “Data protection and safety in distance learning” STAND Handbook was developed for teachers and parents as it contains theory on Data protection and online safety and detailed but simple instructions on how to be safe online. The “Data protection and safety in distance learning” STAND Handbook contains activities for practical implementation at a primary and/or secondary school level. It is aimed at teachers and educators who wish to integrate online safety and data protection in their classroom teaching, in ICT or any other school subject, part of the primary or secondary school curriculum. Also, the Handbook can be effectively used as an independent learning and teaching resource by educators at informal education settings like summer schools, after-school clubs, workshops etc. The Handbook has a flexible and user-friendly structure and content and as a result it can also be used by parents and students so that they can learn more about data protection and online safety. The Handbook targets teachers, parents and students who are not experts at ICT and introduces them to key aspects of data protection and online safety through theory, and activities with detailed instructions.

Learning Objectives for parents and teachers

Through the “Data protection and safety in distance learning” STAND Handbook teachers and parents will:

- learn about fake news and ways to recognize reliable sources of information,
- learn about the European regulation related to the protection of personal data,
- become familiar with the most common digital threats, and learn how to protect themselves, their students, and children,

- learn about the concept of digital identity, differences between personal and Digital Identity and the impact of Digital Identity on our social life,
- develop skills in discerning secure websites for sharing personal data,
- learn about the main harmful phenomena, risks and threats which may occur online and become aware of their consequences to children's well-being and health,
- learn about the rules of netiquette and safe use of the Internet, and gain skills to support their students and children to make safer use of the Internet.

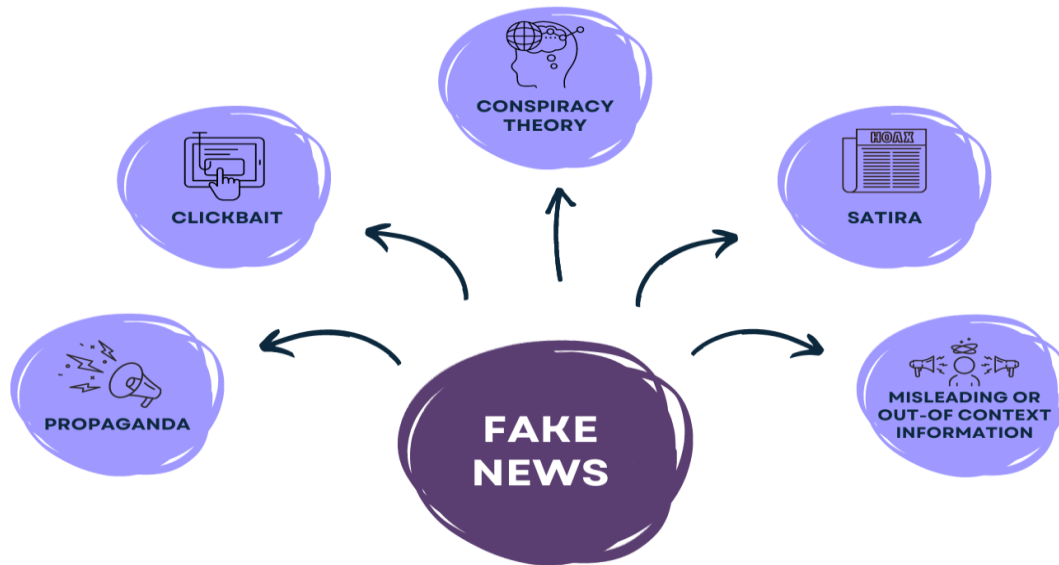
Learning Objectives for students

Through the Data protection and safety in distance learning" STAND Handbook students will:

- learn about fake news,
- learn how to find information from reliable sources,
- become aware of cyberthreats and learn how to protect themselves,
- learn how to identify where, why, and how their data is collected,
- gain knowledge on the European legislation for data protection and learn some key concepts related to personal data,
- become familiar with the concept of and the risks and threats in the online world,
- learn how to behave online and make a safe use of the Internet,
- gain comprehension skills, data literacy skills, collaboration skills, digital research critical thinking, active listening and risk prevention and peer-education skills.

Chapter 1- Critical processing of digital information

This chapter aims to provide guidelines and tips on recognizing and avoiding fake news, finding reliable sources online and safeguarding oneself from infodemic.



Fake news

In Europe, traditional media such as TV, radio, and newspapers are commonly used by citizens to stay informed. However, according to Eurobarometer statistics, European citizens are frequently exposed to fake news daily. The term “fake news” refers to articles that are **purposely incorrect and manipulate people’s beliefs** based on facts and statements of others. To be more specific, in 2023, 70% of the European citizens fully agreed or tended to agree that they frequently came across news and material that was inaccurate or

misrepresented reality (Statista,2023). Fake news can take many different forms as clickbait, propaganda, conspiracy theory, satire, misleading or out-of-context information (Figure 1). The different forms of fake news are presented in the following subsections.

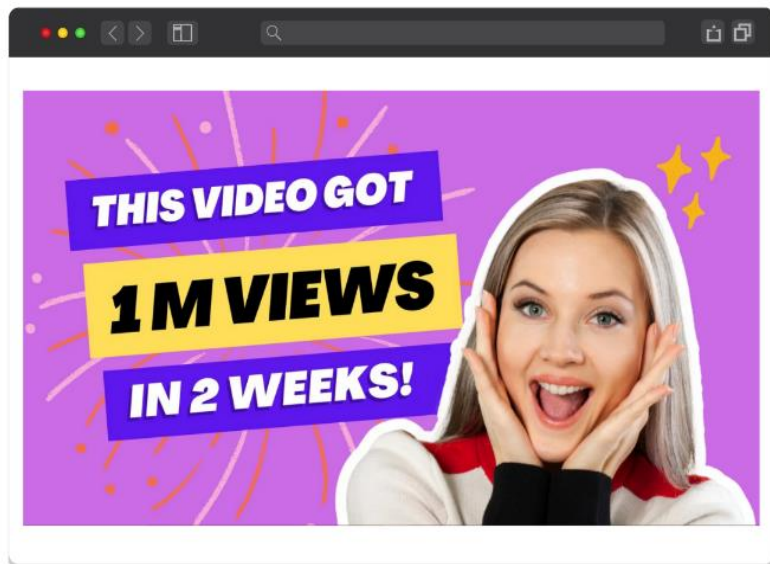


Figure 2. Clickbait on a video thumbnail

(Retrieved from <https://expanderbusiness.com/thumbnail-making/>)

vulnerable to clickbait on YouTube, given that this is the platform they mostly use. It is crucial to educate children on how to recognize clickbait headlines on YouTube. You can see a clickbait example in the picture below:

Propaganda

Propaganda is information that is **purposefully influenced or biased** to support or reinforce a specific ideology. It is often disseminated by political actors with the aim of shaping public discourse. However, propaganda can also manifest itself as fake news, deceiving people by presenting false information that is deliberately designed to seem real.

Clickbait

Clickbait refers to **enticing content**, such as articles or photographs, specifically designed to grab people's attention and compel them to click on a particular website link. The objective of clickbait is to arouse users' curiosity, enticing them to engage with the content by clicking through to the linked webpage. Clicks play an important role in the realm of online media. In fact, the revenue generated by websites heavily relies on the number of clicks they receive. In today's online markets, the use of clickbait has become a thriving strategy as it allows websites to get as many clicks as possible with minimal effort exerted (Munk, 2019). Clickbait news is often misleading, and their headlines can contribute to the spread of fake news on the Internet (Chen et al., 2015). **Clickbait articles and news are prevalent both online and on social media platforms such as Facebook and Twitter.** Children are particularly

Conspiracy theory

Since the first heatwave of Covid-19 conspiracy theories have risen and started spreading in the online platforms continuously. **Conspiracy theories in fact are misleading beliefs** about specific events, facts of circumstances that can be manipulative with negative intentions. These theories often start as a suspicion and spread very quickly via online platforms and social media (European Commission, 2020). The reason behind the development and spread of this kind of fake news is to provoke and manipulate people for political or financial reasons.

Satire

Satire is a form of literary type that uses **humor to comment on an event, a fact, or circumstances** of an individual or a group. However, sometimes satire, or news satire are used to achieve their larger goal of social criticism. Most frequent subjects of satire news are politics and current affairs (Lubeck, 2017). Satire news are usually biased and that is the reason why they belong to the specter of fake news.

Misleading or out-of-context information

Misleading or out-of-context information refers to mostly true facts/ stories that are placed in the wrong context. The most common example of misleading information is an individual's comment that is presented as a fact by the media (UNHCR, 2022).

Infodemic

The World Health Organization (WHO) reports that infodemic or information epidemic includes **false or misleading information during the period of a disease outbreak**. During the covid-19 pandemic fake news on the pandemic were widely spread through mobile phones, internet, and social media. The infodemic was accelerated by social media, spreading false information further and more quickly than a virus (Zarocostas, 2020). The proliferation of misleading information during the COVID-19 pandemic had several negative effects; ineffective treatments emerged, people's mental health and well-being got worse, and people lost faith in medical authorities (WHO, 2022). People's mental health problems

were also triggered by the constant quarantine and the preventive measures that kept them inside their homes, with the only “escape” through the virtual world (Pan-American Health Organization, 2020). In the beginning of the outbreak, it was hard to find trustworthy sources of information, and there was no control of quality on what was written, published, and shared on the web and social media. Below you may see an infodemic example from the COVID-19 pandemic:



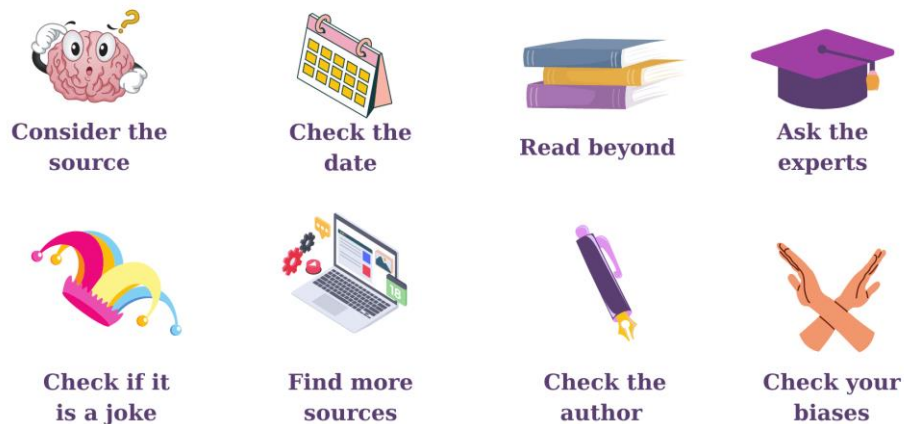
Figure 3. Example of fake news by Greek Hoaxes

(Retrieved from <https://www.ellinikahoaxes.gr/2021/01/30/53-dead-gibraltar-pfizer-vaccine-misinformation/>)

According to this article, 53 people died in Gibraltar 10 days after they were vaccinated with the Pfizer/BioNTech injections. The information presented in the article does not coincide with the official information in the Gibraltar's government (Greek Hoaxes, 2020) and presents misleading content and news based on conspiracy theories.

After the pandemic and the quarantine disinformation and fake news have risen more than ever affecting people's lives, their rights, and the democratic spirit of Europe (European Parliament, 2021). Fake news and disinformation have violated in many cases the fundamental human rights. To be more specific, they violate the right to freedom of thought and to hold opinions without interference (Article 19), also they violate the rights to privacy, as in many cases they can damage an individual's reputation or expose them to personal attacks through hate speech and cyberbullying, violating this way their right to freedom of expression. These violations have an impact on the democratic progress of Europe, as they weaken trust of people in the democratic society and constitution, while they lack trust in the media (Watson, 2023). In several European countries, less than 40% of consumers think that the media can be trusted most of the time (Statista, 2023).

how to spot fake news



Identifying fake news and clickbaits

To shield yourself from fake news, we will present some simple steps and tips (see Figure 4). To identify fake news, you must consider the source that you are reading. Try to click away from the story and think if you have seen it before. Moreover, you need to check the author's credibility and the date that the information you read was published. Furthermore, it is important to check if your beliefs and opinions might bias your decision-making when reading information online, while you need to verify if the information is a joke. You can also consult an expert or a website that spots fake news. Also, you can

search more about the topic that you are interested in and find more sources (International Federation of Library Associations and Institutions-IFLA, 2020).



Teachers and parents should give children tips on their use of social media and especially YouTube. Children should be aware of the click-baits on YouTube and should be instructed on how to avoid them. The following can be signs of clickbait:

- arrows - if they use huge arrows pointing a specific object or place it can be an alert of clickbait,
- capital letters or sentences written in a weird way e.g., WhaT i LearneD Today,
- question/ exclamation marks used in the thumbnail, and
- people in shock pointing a place or an object, and
- headline containing certain words or phrases such as (Shock! / Unbelievable...! BREAKING NEWS.../ SHOCKING..., Click here to.... 5 tips on.... You'll never believe.../ This is what happens if you... etc.).

Figure 5 presents a clickbait example, including most of the signs mentioned above (a person that is in shock, huge capital letters with exclamation marks and an arrow).

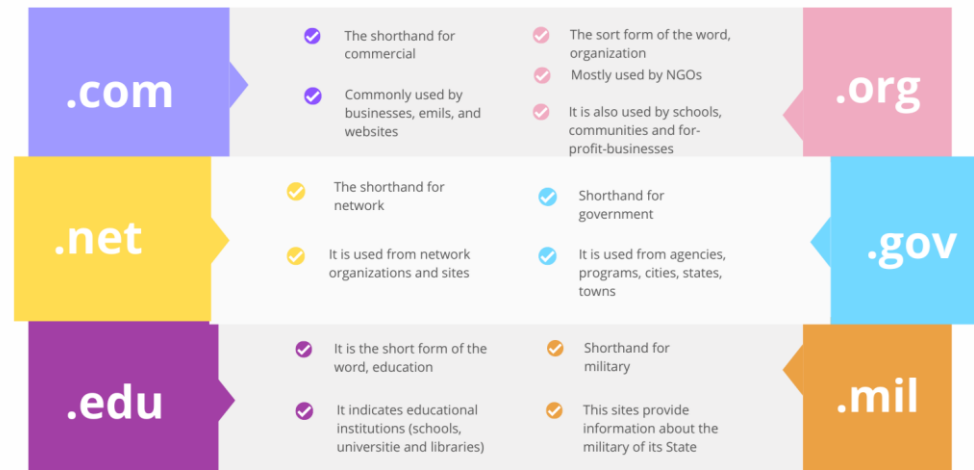
Reliable Online Sources

In today's digital world, it is important for individuals to be able to understand which are the reliable and unreliable sources on the internet. To achieve that, everyone should become familiar with the internet domains and the criteria for evaluating a digital source.

Internet Domains

It is important to give children specific guidelines on how to identify reliable websites when navigating online. Children need to be able to recognize the internet domain of the website. The most common reliable and frequently used internet domains are the following (Figure 6):

Top level internet domains



Criteria for evaluating the reliability of sources

There are many features that can assist someone in determining whether a website is a good resource. You can use the following criteria to identify whether an online source is reliable:

Accuracy- Accuracy is generally the reliability and truthfulness and correctness of an information. To understand if the information provided from the authors is correct, one needs to check the page references or find in general evidence that the information is true (Northern Michigan

University-NMU, 2018). Grammatical and structural errors are very crucial when delivering information. If an article has errors, it indicates that the author either did not pay attention or did not care enough to correct the mistakes. Specific indicators revealing the inaccuracy of a source is the lack of different viewpoints, the lack of date or the existence of an old date meaning that the content is not up-to-date (NMU, 2018).

Objectivity- When bias exists, only one perspective is presented (Arkansas State University -ASU, 2022). Evaluating a source in terms of objectivity can be a challenging process, given that everyone has some degree of bias. However, by employing critical thinking skills, one can become more aware of biased authors and unreliable websites.

Date of publication and currency- It is important to check the date of publication. Most websites usually provide the date that the information was written at the bottom of the page or under the title of the article. Furthermore, at the bottom of a website, you can locate the date indicating the most recent update of the article's content. When searching for historical information, such as dates or past events, you can rely on articles published in previous years. However, for ongoing issues, it is essential to seek out up-to-date sources (NMU, 2017).

Relevance- When assessing the relevance of a source, it is important to acknowledge that it is not feasible to read every possible source pertaining to the desired topic.

Publisher and authority- Internet is an open space where anyone can write about a subject, an event, an idea, or comment on a situation. You can use the following indicators to determine the trustworthiness of an author: author's academic and professional background and reputation and current job position.

Coverage and appearance- Reliable websites have easy-to-read content, photographs that complement the text, music, and the most important evidential working links (NMU, 2018). It is crucial to verify whether the website presenting the information offers a new idea or a different perspective on the topic. Additionally, one should consider the author's intentions or objectives to make an informed assessment of the reliability of the resource.

SIFT & CRAAP Methods

You can teach your students and/or children to read information from reliable resources by familiarizing them with one of the following methods: S.I.F.T. method, or C.R.A.A.P. method. Through the **SIFT method** you can verify the reliability of a resource by following **4 simple steps** (Caulfield, 2019): i) stop, ii) investigate, iii) find another source, and iv) trace claims, quotes, and media of the text (Figure 7). The first step reminds you that when you read something online, you need to stop for a while and check the date, the author, and the accuracy of the website. The next step is to investigate your source, so that you find out whether this resource is worth your time or not. Then, you need to quickly look up other resources on the same topic. This can be done with a quick keywords search. The last step is to try to find the original source so that you can better understand the context and ensure the information is being presented accurately. **C.R.A.A.P.** is the **acronym** for Currency, Relevance, Authority, Accuracy and Purpose (Kurpiel, 2023). In Figure 8 you may find some guiding questions to help you determine the reliability of a source.

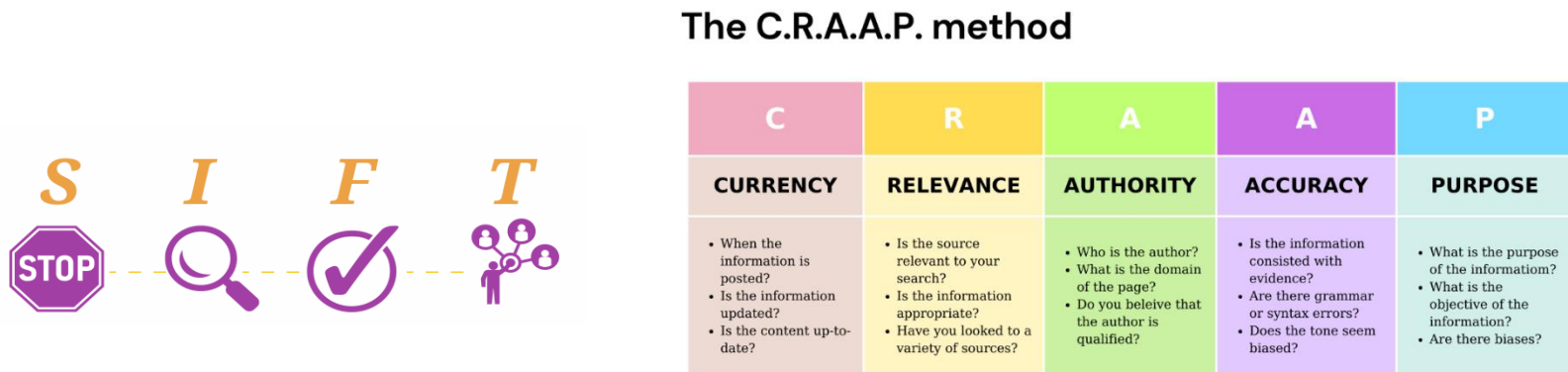


Figure 8. The C.R.A.A.P. method

Retrieved from Kurpiel (2023)

Chapter 2 - General notions on data protection policies

Protecting the data of European citizens is essential for several reasons. In today's interconnected world, where personal information is increasingly collected and processed, safeguarding individuals' data has become a critical priority. Such is the priority that the European Union agreed to create regulations regarding it that all countries would have to apply, thus the GDPR (General Data Protection Regulation) was born. The GDPR was created with the aim of strengthening and unifying the data protection of EU citizens. It was implemented on May 25, 2018, to replace the 1995 Data Protection Directive and became the most comprehensive and applicable privacy regulation in the EU to date. It was designed in response to rapid technological advancements and the need to update and modernize existing data protection laws. The GDPR defines individuals' fundamental rights in the digital age, the obligations of those processing data, methods for ensuring compliance or sanctions for those in breach of the rules. In this chapter, we will cover the main aspects of the GDPR and its integration into national legislations. Then, key terms as consent, cookies, etc. will be explained. After that, we will present the fundamental obligations of the GDPR for processing data. Finally, we will explore the rights related to personal data detailed in the GDPR. These rights include, among others, the right of access, which allows individuals to request information about how their personal data is being used; the right of rectification, which allows them to correct inaccurate data; and the right of erasure, which gives individuals the possibility to request the deletion of their data in certain circumstances.

Introduction to GDPR and national laws

GDPR was created to replace the 1995 Data Protection Directive used across various European countries. The 1995 Data Protection law allows each country to control and customize its own privacy laws. This makes it harder for businesses to introduce their service between countries since they would have to refer to multiple privacy requirements and keep up with all of them. After the internet became commonplace, the EU parliament decided they need a new guideline that adapts to a more connected world where data is the common currency. The GDPR is designed

Country	Own national registration
Spain	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. <i>Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights" (LOPDGDD).</i>
Italy	Codice in materia di protezione dei dati personali. <i>Code on the Protection of Personal Data.</i>
Greece	Law on the Protection of Personal Data.
Poland	Ustawa o ochronie danych osobowych <i>Act on the Protection of Personal Data</i>

Figure 9. National Legislations based on the GDPR

Created by Blue Room Innovation. Copyright 2023 by Blue Room Innovation.

- Spain: The data protection law in Spain is known as the "Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights" (LOPDGDD)
- Italy: The law on data protection in Italy is known as the "Codice in materia di protezione dei dati personali" or "Code on the Protection of Personal Data."
- Greece: The data protection law in Greece is known as the "Law on the Protection of Personal Data"
- Poland: The data protection law in Poland is known as the "Act on the Protection of Personal Data" (Ustawa o ochronie danych osobowych).

GDPR terms and definitions

In this section, we will present some key GDPR concepts:

Data subject- an individual, a resident of the European Union, whose personal data needs to be protected. You, reader, are a data subject.

to better fit modern technologies and practices (Comisión Europea, 2017). The GDPR is a **regulation directly applicable in all member countries** of the European Union, which guarantees greater uniformity and consistency in the application of data protection regulations throughout Europe. The different countries have transferred the GDPR to their legislation in the following documents (see Figure 9):

- Spain: The data protection law in Spain is known as the "Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights" (LOPDGDD)
- Italy: The law on data protection in Italy is known as the "Codice in materia di protezione dei dati personali" or "Code on the Protection of Personal Data."

Personal data- Personal data refers to any information that is about a person who can be directly or indirectly identified. This can include details like their name, identification number, location data, online identifiers, or even certain factors that are unique to them, such as their physical or mental characteristics, genetic information, economic situation, cultural background, or social identity (see Figure 10).

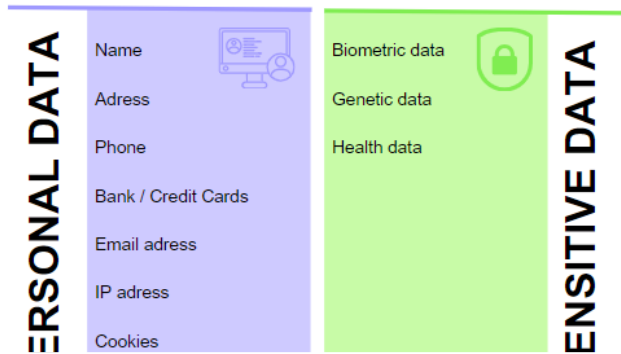


Figure . Examples of personal and sensitive data

Created by Blue Room Innovation. Copyright 2023 by Blue Room Innovation.

Sensitive data- The following personal data is considered "sensitive" and is subjected to specific processing conditions: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical convictions, union membership, genetic data, biometric data processed solely to identify a human being, data relating to health, data relating to a person's sexual life or sexual orientation (see Figure 10).

Data processing- Data processing refers to any action or group of actions carried out on personal data, whether manually or automatically. These actions can include collecting, recording, organizing, storing, modifying, retrieving, using, sharing, transmitting, publishing, aligning, combining, restricting, deleting, or destroying personal data.

Consent- Consent of the data subject refers to a clear indication, given freely and with knowledge, where the individual expresses their agreement for their personal data to be processed (Information Commissioner’s Office, 2023). This can be communicated through a statement or a positive action that shows their explicit and unambiguous agreement to the processing of their personal data.

Cookies- cookies are small files that are stored on the computer or device when visiting a website. Imagine that they are like little notes that are kept remembering important things. These notes contain information about subject visit to the website. There are different types of cookies. The ones below are the most common:

- **Session cookies-** They are like temporary notes that are deleted when the data subject close his browser. These cookies are used to remember the activity while browsing a website. For example, if the subject is shopping online, session cookies help him keep items in his shopping cart until he decides to check out.
- **Permanent cookies-** Unlike session cookies, these are not deleted when the data subject close his browser. They remain on the device for a longer period. Persistent cookies can be useful for remembering preferences when the subject returns to a website, such as the preferred language or accessibility settings.
- **Third-party cookies-** These cookies are placed by companies other than the website visited. They are frequently used to collect information about browsing habits and serve personalized advertisements. For example, if the subject visits a shoe website, he may see advertisements for shoes on other websites that he visits later.
- **Analytical cookies-** These cookies are used to collect information about how users interact with a website. They help site owners understand which parts are most popular, how much time visitors spend on each page, and which links they click. This information helps to improve the user experience and make the website easier to use.
- **Advertising Cookies-** These cookies are used to display relevant ads to the data subject. They remember which websites he has visited and share this information with advertising companies. This allows them to show advertisements that may be of interest to the subject based on his interests and online activities. It is important to know that cookies cannot damage the computer or steal personal information. However,

it is essential to be aware of how they are used and have control over them. The data subject can adjust the cookie settings to allow or block certain types of cookies according to preferences.

GDPR obligations for processing personal data

The GDPR establishes a series of principles and obligations for organizations that process personal data, whether they are companies, government organizations or non-profit entities. Some of the key provisions of the GDPR include:

- **Informed consent**- Organizations must obtain the explicit consent of individuals to process their personal data and must clearly disclose the purpose of the processing. This is the reason why today the forms to collect data on a web page are more complete. The data processor must also request express consent when physically request data to enter it into a digital database. When accessing a website, data is also collected through cookies, therefore, whenever a website is accessed, the message to accept, configure or reject cookies appears. All the information regarding privacy and cookies can be found in the privacy or cookie policy sections that websites usually have. In the case of granting the data physically, they must explain the privacy policy in the document.
- **Accountability and Transparency**- Organizations must be transparent about how they handle personal data and must implement appropriate security measures to protect that data. GDPR explicitly says that it should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the process and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed.

GDPR user rights

In the digital age, data processing has become ubiquitous and increasingly difficult for individuals to understand. Individuals have the following rights over the processing of their personal information:

- **Right to access**- The right of access grants individuals the authority to acquire a copy of their personal data along with additional supporting details (Information Commissioner's Office, 2023). It enables individuals to comprehend how and why their data is being utilized and verify that it is being done in a lawful manner (Information Commissioner's Office, 2023).
- **Right to be informed**- Processing controllers have a duty to notify individuals about their intended use of personal data when collecting it. This obligation exists regardless of whether the data subject requests the information or expresses interest in it. Controllers must proactively fulfill this obligation, ensuring that individuals are informed about the processing of their data.
- **Right to be forgotten / erasure**- An individual should have the right to correct their personal data and have a 'right to be forgotten'. Specifically, the individual should have the right to have their personal data deleted and no longer processed in cases where the data is no longer necessary for its intended purpose, the individual has withdrawn their consent or objected to the processing of their data, or the processing is not in compliance with the regulations. This right is especially important when a child has given consent without fully understanding the associated risks and later wishes to remove their personal data, particularly from the internet. The individual should have the ability to exercise this right even after reaching adulthood. To enhance the right to be forgotten in the online realm, the right to erasure should be expanded so that a controller who has made personal data public is obligated to notify other controllers who have processed the same personal data to delete any links, copies, or replicas of that data.
- **Right to data portability** - the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services (Agencia Española de Protección de Datos, 2018). It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability (Agencia Española de Protección de Datos,

2018). This enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.

- **Right to rectification-** Individuals have the right to have any incorrect personal data corrected. In certain cases, a simple request from the data subject, such as fixing a name spelling, updating an address, or changing a phone number, will be enough for rectification. According to EU regulations, inaccurate personal data must be rectified promptly and without unnecessary delays. However, if the requested rectifications are related to legally significant matters, such as the individual's legal identity or the accurate address for legal document delivery, mere requests for rectification may not be sufficient. The controller may require evidence to substantiate the alleged inaccuracies. However, such demands should not impose an unreasonable burden of proof on the data subject and should not prevent them from rectifying their data.
- **Right to restriction processing-** data subjects can temporarily restrict a controller from processing their personal data (Council of Europe, 2019). Data subjects can request the controller to restrict processing where the accuracy of the personal data is contested, -he processing is unlawful and the data subject requests that the use of the personal data be restricted instead of erased, the data must be kept for the exercise or defense of legal claims, a decision is pending on the legitimate interests of the data controller prevailing, over the interests of the data subject (Council of Europe, 2019).

Chapter 3- Digital Threats and Cybersecurity

This chapter aims at providing some important information about the threats that may occur when using ICT systems at school. As schools today rely on digital technologies it is important to be aware of the threats that come along with its usage. This chapter will present the most common threats nowadays and the measures to protect against them that schools can undertake.

Cybersecurity in the education sector and common digital threats

ICT refers to Information and Communication Technologies and it can be defined as a set of **technological tools and resources** that can be used **to create, store, share, and exchange information**. School uses these different ICT tools on an everyday basis and they bring a lot of benefits like improving learning efficiency and interactivity, less work for teachers, and increasing students' motivation, to name just a few. Yet, today with schools relying a lot on using these tools and moving towards the remote learning and hybrid models the risks associated with using them become ever greater. School today is exposed to various cybersecurity threats. Let's learn about the most common ones in this chapter.

Phishing

Phishing is a form of **cyberattack**, where there is an attempt to obtain some sensitive information from a victim. The offender very often impersonates a trusted institution or a person of social trust with an authoritative position. An example here will be forcing someone to log in to a bank account with their sensitive data and authorize data. Examples of phishing attacks that might appear will include sending an SMS message with an attachment that the receiver is meant to click on. The link is infected and results in downloading of malware that encrypts data. Criminals send messages to many random numbers. The aim of the attack is to extort money. Fake SMS may inform, for example, that there is a need for the payment of a small amount missing for the invoice of the electricity, gas, water, internet, telephony, etc. operator or Tax office with a refund or underpayment of tax. And, of course, criminals try to adapt the content of their attacks to the current situation in the country,

the mood, or ongoing events. Another example is the vaccination issue and the fake text message about the need to pay a surcharge for the vaccine or encourage people to register (for a fee) for the vaccination. The amount that is requested is usually small. Criminals hope that the receiver will not verify in detail whether the amount due is legitimate. It very often turns out that the amount of money lost is greater than the one mentioned in the text message. Phishing messages also spread on social media and online communicators (E. P., 2022).

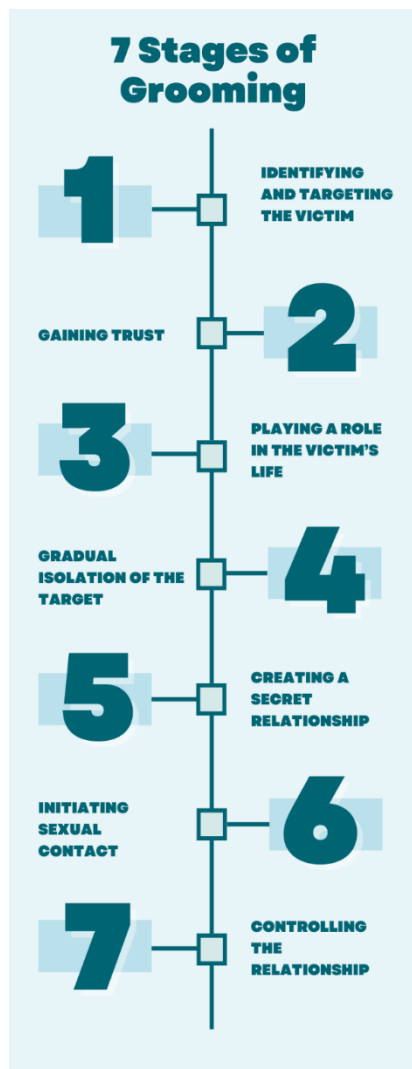
Online predators

The internet, except for its great potential, is the place where people can act anonymously and hide their identities. They often pretend to be someone they are not. **Online predators are the users of the internet** that seek contact with children and adolescents for abusive, sexual, and violent purposes. Their actions can result in harming the victims either online or offline. Online predators operate on social media, forums, instant messengers, and chat rooms. They seek places where they can reach young people. They try to befriend young people and initiate contact so they can get their attention. Next, their aim is to establish some kind of emotional connection with a child so that it will be difficult for the young person to recognize that they are speaking to someone who can have bad intentions towards them.

The grooming process is the process when there are actions undertaken by an online predator to establish a friendly relationship with a victim to lower their inhibitions. Sometimes the grooming process also includes adults from the child community. In this way, a predator is taking all the steps to gain trust. They know what is trendy now and what youngsters are interested in, for example, fashion, music, or any current trends, etc. Children are prone to grooming attempts as they may look for information about sex and any similar information on different websites.

The grooming process can follow the stages below (De Marco, 2017) (see Figure 11):

1. **Identifying and targeting the victim**- online predators identify and start grooming their potential victims based on their personal and sexual desires. They carefully select those who they think they may have the most success with and they feel confident that they can groom them.



2. **Gaining trust-** online predators will choose to pretend the roles that they feel will gain the trust of the victim like volunteers, teachers, trainers, or priests. Such people inspire trust and develop a special type of rapport with children. They may present the child's parents as opponents so that the child feels that they need a predator to give him some comfort. Sometimes, they also act childish aiming at developing relationships with a group of children.

3. **Playing a role in the victim's life-** predators will often try to convince the victim that they understand what he/she feels the best. They shower the child with the attention that they know he or she needs. In this way, a special trust is built. This is when the victim may start lying to their parents and spend lots of time talking to the predator.

4. **Gradual isolation of the target-** After gaining trust and making sure that the child needs their relationship the child begins to be isolated by the predator. This prepares the child to begin sexual contact with the predator. There might be some suggestive talk happening on social media as well as face-to-face meetings.

5. **Creating a secret relationship-** the predator convinces the victim to keep the relationship a secret and that other people will not understand this. They underline that revealing the secret may have bad repercussions.

6. **Initiating sexual contact-** after the relationship is secured with the victim the predator will initiate sexual contact with the child.

7. **Controlling the relationship-** as the wrong relationship develops the predator knows that what he/she is doing is wrong and the relationship needs to be kept secret.

Figure 11. Process of Grooming a Victim

(Adapted from De Marco, 2017)

Identity theft

Identity is the personal data of a person that allows that person to be identified. Identity theft occurs when another person comes into possession of this personal data to use it against the owner's will. Criminals most often seek to obtain data that will include: first name, surname, date of birth, address of residence, credit card number. The consequences of identity theft may vary from minor ones to serious financial and reputation loss. Identity theft takes place through phishing or hacking, sharing passwords with untrustworthy individuals, or having personal data breached in the institution. This can also be done to register for a competition or a newsletter. Often data theft takes place through fictional websites when unaware users share their personal information. A very common way for students to have their identities stolen is by creating fake profiles on social network platforms using their data, photos, and interest information. Fraudsters can use these profiles by impersonating students' identities and committing various types of offenses. Where criminals gain access to students' data, they can take out loans, enter into contracts for services or attempt to defraud parents by posing as a student or other family members. Unauthorized access to school accounts and online services is another threat that can lead to students' identities being stolen. Criminals who hack into such accounts can access a variety of information about students, such as their grades, homework, personal information, or contacts with other students and teachers. Such activities can lead to a range of negative consequences, such as grade manipulation, theft of work, and damage to a student's reputation by publishing inappropriate content on their behalf. This also imposes risks on a student's family as it may bear the costs resulting from the fraudster's criminal actions. Damaging students' and families' reputations can affect relationships with peers, teachers, and future educational and career opportunities. As a result, students can become victims of cyberbullying and harassment from individuals who use their personal information for destructive purposes. This can lead to emotional problems such as anxiety, depression, or social isolation. Finally, identity theft can lead to a loss of trust in educational institutions, teachers, or peers which can affect student's motivation to learn and take part in school life.

Malware

The term “Malware” comes from “malicious” and “software”. Malware is a term used to describe any type of “**malicious software**”, which is designed to damage a computer, computer system, network, tablet, and mobile devices by taking control over its operational system. There are different types of malwares that criminals use (Harford, 2018):

- **Computer worms**- self-generating computer programs that may infect the computer by copying their functions.
- **Computer virus**- a piece of code that inserts itself into a code of another program and makes it undertake malicious actions and spread itself.
- **Trojan horses**- it downloads into a computer and disguises a legitimate program.
- **Spyware**- it works by collecting information about user activity, such as pages visited on the internet.
- **Browser hijackers** - make changes to the configuration of browsers (e.g., add toolbars or change the start page).
- **Rootkit** - a hidden application that allows the administration of the entire system, e.g., to steal data.
- **Keyloggers** - this software works by reading and then recording the keys pressed by the user; this allows cybercriminals to steal passwords, e.g., for online banking, and social media accounts.

When the computers or network is affected by malware there might be some unwanted advertisements that appear on the screen and by clicking on them, we may download even more malware. Computers may also be affected by Spyware which will collect information about the activities of users without their knowledge and consent. Information like passwords, payment information, or photos are gathered and might be used for fraud (O'Brien, 2021).

Privacy breaches

Schools typically hold a large database of the students' personal data information. They are used for maintaining records and automating processes, yet they also create a target like a data breach (Irwin, 2018). A data breach occurs when a fraudster gains unauthorized access to a school database and all sensitive information within it. Personal data can be lost or stolen, destroyed without consent, altered without consent, or accessed by someone who is not authorized to use it. This can result in selling the data obtained and using it for further crimes. It can result in the exploitation of the school's finances as well as damaging its reputation. It is important to mention that although the loss of data of younger students seems not to impose any bigger risks it can create issues in the future when they are adults. All organizations that process EU residents' data must comply with GDPR rules. It gives individuals more power over the personal details being shared. Examples of a data breach include (Irwin, 2018):

- **Unauthorized access**- students or unauthorized members of staff will use the teacher's laptop and will gain access to saved files. Teachers may also have some autosaved login details for their accounts or email, and it gives the user access to much more information.
- **Deliberate or accidental action**- an old PC might be sent to be destroyed without wiping the hard drive or throwing away documents without having them shredded first.
- **Alteration**- unauthorized access to the school payroll system and entering false information about staff pay grades.
- **Accidental disclosure**- sending an email containing the personal information of a student to the wrong recipient.
- **Loss of availability**- schools might lose access to information that is only available electronically due to power cuts.

Cybersecurity Measures and Technologies

Managing data security at schools has become an important issue in recent years. The learning taking place remotely has also added level to the data security precautions that need to be taken nowadays. Unauthorized access to sensitive and personal information can be very harmful to pupils, parents, and staff. This is why educators need to pay much attention to the security systems used in their institutions. Let's explore the ways how can school protect against cybersecurity attacks and what impact they may cause on schools, pupils, and parents.

What are the impact and implications of cybersecurity attacks?

Cybersecurity attacks can have an enormous impact on school's every day's life. This impact may influence teachers, pupils, and parents. Schools are particularly exposed to risks related to online safety. These risks include:

- **Ransomware**- a kind of cybersecurity attack when the user clicks a bad link which downloads dangerous malware into a computer system. This may happen when you open an attachment in an email or click on a link to a malicious website. The email may look perfectly fine and draw no suspicion that it contains a virus. The attachment downloads an aggressive program that delivers ransomware onto the used device and throughout a school computer system it may encrypt all the files and make them inaccessible until a certain amount of ransom is paid to the attackers. Schools store a large amount of data with personal information regarding all students, teachers, and staff. This information can be used for financial crimes and sold on the black market. Schools are a big target here as they usually rely on antivirus software only. Universities usually have a special system in place that guards them against these attacks.
- **Human error**- people working at school may not fully understand the scale of cybersecurity that should be implemented. It is usually pupils who are taught how to stay safe online, yet it should be adults who need training too.

- **Business email compromise**- an attack when an attacker learns about some important school information and uses it to make the school pay money to avoid this sensitive data leaking. Fraudsters can pretend to be suppliers and ask to pay money into a different account than usual and give a trustworthy reason. They may target a new member of staff who is not yet experienced to spot the signs of a scam.
- **Internal data breaches**- there are human error accidents that may lead to sharing sensitive data like sending an email containing important data to a wrong address or losing a USB stick.
- **Internet of Things**- it is important to remember how many objects are connected to the internet or a network of devices. All devices need to be secured. If not, fraudsters can access them all when they get access to a network.

Ways to prevent cybersecurity attacks

There are various ways in which schools may prevent cybersecurity attacks. Firstly, cybersecurity needs to be constantly checked, updated, and evaluated. Educators and school staff need to be offered training opportunities. Teachers and students need to know when they are using certain data and keep track of this. They may, for example, provide their full name when signing into Facebook or other social media platforms. VPN and anti-tracking services need to be incorporated into these measures too. Set up a 'data breach' or 'data leak' Google alert so that you will receive information if any new services or websites have suffered a leak within 24 hours. If the accident of leaking some information happens, contact school administrators and IT staff who can deal with the situation. You may also ask students to update their passwords straightaway. Each school is advised to implement a multi-layered security strategy. It is a tool that may prevent data breaches ahead of time. In Figure 12 you may see security strategies for data breaches. In Figure 13 you can see simple ways for keeping your data secure at school and in Figure 14 you may see some tips for students to protect their privacy online. What school needs is a plan beforehand just in case there is a problem to take precautions.



Figure 12. Security strategies for data breaches.

Adapted from (Gutiérrez, 2023).

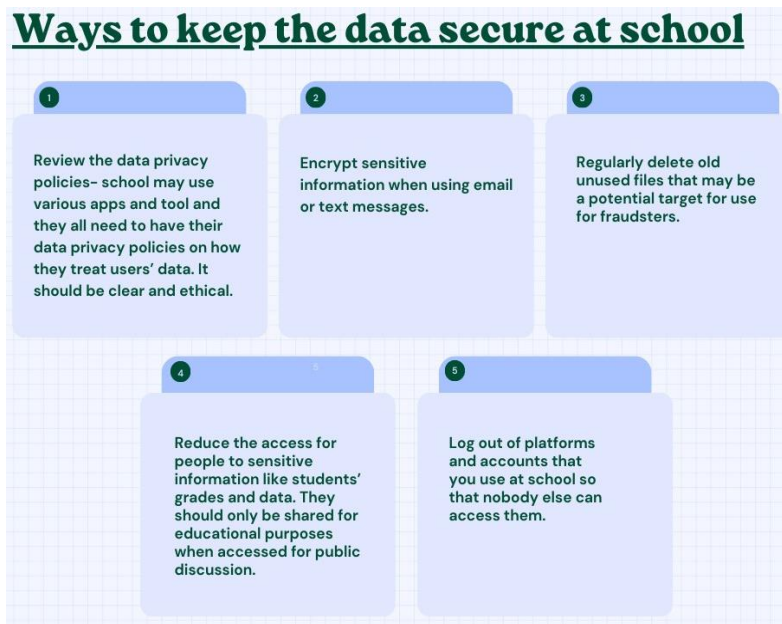


Figure 13. Ways to keep the data secure at school

Adapted from (Gutiérrez, 2023).



Figure 14. Tips for students to protect their privacy online.

Adapted from (Gutiérrez, 2023).

NEW EMERGING CYBER THREATS	
Distributed Denial of Service Attacks	these attacks will prevent users from accessing data. What happens very often is attackers overloading the network infrastructure and making the system unavailable. It affects mobile networks and connected devices. Sometimes students get involved in these attacks as they want to avoid taking the test or attending classes
Zoom bombing	the Zoom online meeting is interrupted by attackers who will share obscene material, and assault students verbally and the aim is for the session to end
Disinformation	the use of social media and online media has resulted in some fake information spreading easily across the Internet. The aim of this is to create uncertainty and scare people. In education, this can affect teachers who might use false information if not checked properly. Deepfakes are photos, videos or audio when people's face, body or voice has been altered through artificial intelligence. It attempts to manipulate and spread fake information. Educators need to be trained to detect deepfake to protect students against disinformation
Man-in-the-middle attacks	allow an attacker to eavesdrop on data being sent back and forth between two people, networks, or computers. The cyber-attack takes its name from the fact that the attacker is 'in the middle' or between two parties attempting to communicate. In effect, the attacker is spying on the interaction between the two
Nigerian scam	The sender asks for help, usually in the form of an email, in facilitating the transfer of a sum of money. In return, the sender offers a commission - a large amount, sometimes up to several million dollars. The scammers then ask for money to be sent to cover some of the costs associated with the transfer. If the money is sent to the fraudsters, they disappear. Alternatively, the fraudsters try to get more money by claiming that there are still problems with the transfer

Figure 15. New emerging cyber threats to the educational sector.

(Adapted from Colaco, 2022)

personal identity, as the attributes and characteristics that define an individual in the physical world are different from their digital representation. Personal Identity mostly refers to the genetic characteristics of an individual while Digital Identity is the behavior and interaction in the digital world. Personal identity refers to someone's name, surname, birthday, academic educational level etc. On the other hand, Digital Identity could be the footprints that someone leaves on internet, a password, interaction with other users and comments on social media, even what someone buys online. In contrast to personal identity, which is typically difficult to change, someone's Digital Identity can vary across different browsers and websites (Rand, 2021).

Other emerging cyber threats to the education sector.

Cyber threats constantly evolve with the development of digital technologies. In Figure 15 you may find some of the emerging cyber threats.

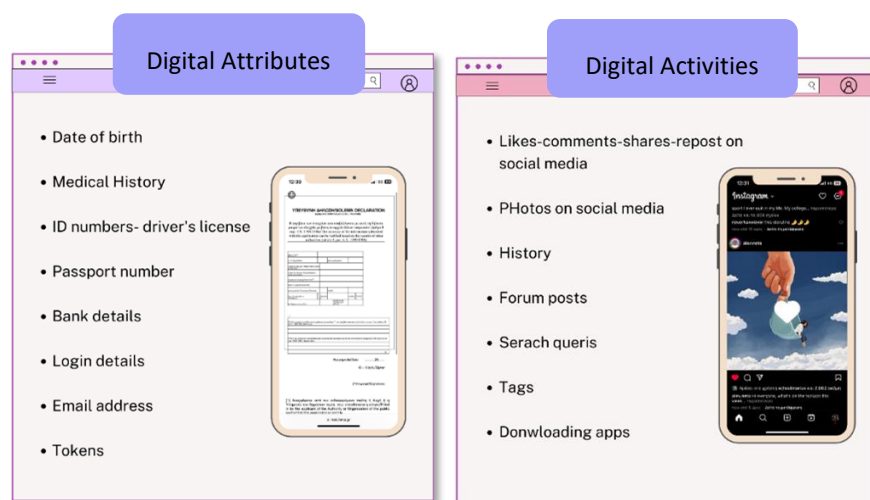
Chapter 4- Digital Identity

In the physical world, presenting personal identification is crucial to establish one's personal identity in various scenarios such as entering places like a bank, a post office, or a police station, or when taking exams at school or university. Individuals are required to carry their personal identity documents for verification purposes. In the digital world, the process of identification is significantly more complex and distinct. **Digital Identity differs greatly from**

This chapter aims at providing guidelines and tips to teachers, parents, students, and school staff regarding their digital identity. To be more specific, this chapter presents the definition of digital identities, the difference between personal and digital ID and the impact of digital ID on our social life. Finally, in this chapter good practices of using Digital Identity in schools are presented.

Definition of Digital Identity

The Digital Identity consists of two categories: the digital attributes, and the digital activities (DeNamur, 2022). **Digital activities** refer mostly to comments, likes, shares on social media, post and search on the web, or apps used on daily basis, while **digital attributes** refer to more personal information such as an email address or login passwords and usernames (DeNamur, 2022). More details can be found in Figure 16 below:



How Digital Identity affects our social and daily life

In today's world, people rely on digital devices extensively in their day-to-day lives, whether it's browsing social media or utilizing government services for tasks like filing taxes applications (World Economic Forum, 2018). Online interactions leave behind digital trails and create a comprehensive history of personal choices, effectively mapping users' attitudes, and behaviors in the online world. Digital trails can be left in various sectors, including healthcare, social platforms, commercial stores, travel and food, financial services, and telecommunications (see Figure

17). Based on the data of the European Parliament, 80% of the EU citizens use digital tools to access public services, while until 2030 this will also take place in countries outside the EU (European Parliament, 2023).



Figure 17. Digital Identity in our everyday lives.

Adapted from WEF (2018)

The digitalization of identities has brought numerous positive impacts to citizens, companies, and public administrations. First, by embracing digital identities, citizens can enjoy enhanced convenience, efficiency, and security in their interactions with various entities, for example, they can manage their own healthcare, take a loan, open a bank account on their own, shop and even vote. When it comes to companies, they can provide enhanced customer experience, by capturing and analyzing customer data through

digital identities and by offering stronger security measures (WEF, 2018). Regarding public administration, they do not have to deal with workload; they can be flexible and give better instructions to the individuals (IDcentral, 2023). However, people who want to stigmatize a person or brand by spreading false information on social media frequently take advantage of loopholes related to digital identification. The 'Internet trolls' do that. To provide additional details, internet trolls can be described as individuals who purposefully engage in online behavior with the intent to create conflict, offend others, and display hostility on social media platforms (GCFGlobal, 2023). These people are challenging to spot since they frequently construct one or more false profiles to try to damage a firm's reputation or occasionally just to embarrass a company or a person (Arimetrics, 2022).

How to protect our Digital Identity

In today's digital world, the importance of safeguarding our digital identities cannot be overstated. Whether we are logging into our social media accounts or accessing our bank accounts, the potential risks of identity fraud loom large. It is imperative that we take proactive measures to protect ourselves and our sensitive information. Some of them are (see Figure 18):



Figure 18. How to protect your Digital Identity

Adapted from Edwards (2020)

- **Verify the address of the website-** If a website utilizes a lock symbol in the URL, it indicates that it is safe to share data as the site is encrypted. However, if the lock symbol is absent, it implies that the Digital Identity is at risk and vulnerable to potential threats (Balaban, 2021).

- **Use VPN-** The Virtual Personal Network, or else VPN, is a software that protects you by covering your IP addresses when you are searching and navigating on the web. Basically, VPN is a good way to be encrypted all the time (Edwards, 2020), as it can “relocate” your address and have access for different servers. Therefore, your identity even if you are using public Wi-Fi is always protected and secure (McCann, & Watts, 2023).
- **Improve passwords-** It is crucial to create strong and unique passwords, or to have a password manager like the one that Facebook uses when entering to other social platforms of Meta. The password manager will ask you to change your password regularly and will tell you if your password is strong enough or not, while they protect you from fishing and other threats.
- **Set anti-tracking software-** You can also be protected by setting anti-tracking software. Moreover, it is important to be cautious with the information that you share online on your social media. It is suggested not to give information about your private and family life. Also, you should avoid using public Wi-Fi connections (Edwards, 2020).
- **Review your content before uploading-** Make sure that you carefully review your content before sharing it on social media. Take a moment to read your post twice allows you to consider the potential impact they may have on others, as well as evaluate any unintended consequences. One good practice to be protected is to consider whose front page you would like your post to appear on.
- **Clear browser’s history-** you should always clear your history on the browsers (ISTE, 2015). Browsers typically store your browsing history, personal data, and preferences. As a result, by clearing this information, you not only make it harder for others to track your online activities but also enhance your browsing speed (ISTE, 2015).

School and Digital Identity: good practices

Digital Identity and the use of it in schools today is a great advantage. With the use of the digital ID nowadays, it is easier to verify the person that is visiting the premises of a school. Schools can also make the management of the school simpler. The registration of children can be faster, while school administration can easily access important student information. Moreover, it is easier for the teachers to prepare a lesson plan and

share it with their students, to track their progress and assign them activities (SchoolPass, 2022). A good practice that the schools may implement as beneficial in addressing Digital Identity Issues is the Learning Management System (LMS). LMS is basically a software that gives the opportunity to not only store your materials in a location and avoid risks of data loss but also to ensure that student data is safe and secure. Moreover, with the use of LMS educators could monitor student's activities and address their online behavior (Soni, 2023).

Chapter 5- Online behavior – rules, risks, and advice

The use of the Internet has become nowadays almost indispensable in daily life and has deeply changed the way people inform themselves and interact between each other. Digital and online tools have been increasingly used also in education as a support for teaching and learning. Examples include online classes, assignments organized through apps, online sources that teachers use for teaching (e.g., videos, research paper), and chat groups with classmates. Especially during the COVID pandemic, the Internet and the use of digital tools allowed the school system to continue to function, connecting teachers and students in distance learning. Along with the positive aspects (e.g., speed and flexibility of communication, access to unlimited information), potential risks have also emerged, and kids are often more exposed and less prepared to face them. Various threats and incidents that could happen on the internet could lead parents to question whether the Internet is safe enough for their children and what is the best way for them to develop a healthy and functional relationship with it. It therefore becomes essential to raise awareness about these topics, to know what the most appropriate behaviors are to put in place when using the Internet, both to avoid possible threats and to ensure the well-being of all users. This chapter aims to promote knowledge for teachers and parents to be fully equipped to support children in using the internet consciously. To this end, the chapter will investigate the most prominent risk phenomena in which young people may be most exposed and the ones that can be most harmful to their health and well-being. We will discuss some tips and advice on good practices and behaviors to be adopted, following the rules of "netiquette" (good etiquette concerning the Internet). Based on these rules, the final part will focus on advice for parents and teachers on how to support children and students to exploit the Internet to its full potential, safeguarding their interest and promoting their knowledge. In the last part, an activity will be introduced for teachers to use within a class group with respect to online behavior in all its facets.

Online behaviors, risks, and legal consequences

Internet is not a place of total freedom, without rules and detached from the “real” world, but in fact behaviors in digital environments have effects and implications also in the real life, including psychological consequences, emotional and physical ones but also legal (not everything is legitimate on the internet and often people and especially kids are not aware of this). It is important to understand that online and offline worlds are connected and affected one another and that there are risks of becoming victims but also of committing illegal acts (Nowicka et al., 2023).

Main risks, threats, and harmful phenomena in the use of the Internet

To raise awareness about potential harmful phenomena and threats kids may face, it is necessary to improve knowledge of all the risks and cases that may happen on the internet, and possible consequences. It is useful to specify that some actions that occur online have emotional and psychological effects until physical ones for the victims, but also – often not considered – legal consequences for perpetrators, even if these lasts can differ with respect to different considered country. To this end, we would like to give a general overview of the most prevalent and current **threats**.

- **Child Pornography** is any visual depiction of a minor (a person who has not reached the age of consent) engaged in sexually explicit and implicit activities. Such depictions may be in the form of photographs, films, videos, images, or computer-generated images. For young people, it is helpful to know that possessing and sharing material about other minors (e.g., a classmate, a friend, an unknown person) also falls into this category (Zurcher,2023).
- **Cyberbullying** refers to intentional and repeated harm inflicted through the use of digital devices. Cyberbullying can occur through text messages, texts, and apps, or online in social media, forums, or games where people may view, participate or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or

private information about someone else, causing embarrassment or humiliation. It is important to know that cyberbullying behaviors are characterized by four important elements: a) it is *intentional*, b) it is *repetitive*, c) it is *harmful* to the target, and d) use of *digital devices* (which is what differentiates cyberbullying from bullying) (Mubasher, et al., 2023; Nowicka, et al., 2023; Yemima, 2023).

- **Cyberstalking** is a crime in which someone harasses or stalks a victim using electronic or digital means, such as social media, email, instant messaging (IM), or messages posted to a discussion group forum. Cyberstalkers take advantage of the anonymity afforded by the internet to stalk or harass their victims. Examples of cyberstalking actions include: monitoring the victim's online-and, in some cases, offline-activities; tracking and following the victim's location online or offline; intimidating, frightening, controlling or blackmailing the victim; etc. (Mubasher et al., 2023).
- **Denigration** refers to "dissing" or "gossiping" online about someone by writing and spreading vulgar, derogatory, cruel, mean or false rumors, having electronic communication devices as the medium. An online disparaging comment is typically posted as a malicious viral rumor to harm the victim (Yemima, 2023).
- **Exclusion** is a kind of online ostracism or social sabotage that occurs when a user is intentionally excluded from a community, chat, or interactive game (Agustiniingsih & Yusuf, 2023; Yamina, 2023).
- **Hikikomori**: literally "isolating oneself." This is a form of social withdrawal, which occurs when a person uses the Internet as the only means of making direct contact with the outside world (<https://www.hikikomoriitalia.it/>).

- **Grooming** occurs when someone builds a relationship, trust and emotional connection with a child or young person so they can manipulate, exploit, and abuse them (Kasar, et al., 2023). For more information you can read Chapter 3 - Digital threats and cybersecurity (Figure 11).
- **Impersonation** -involves a person using an identity other than their own for malicious purposes. Using someone else's identity is a powerful tool for damaging reputations and harassing others. An account made under someone else's name, especially if it is a trusted individual, can be used for everything from cyberbullying to phishing to extortion (Agustinarsih & Yusuf; 2023).
- **Internet addiction**- It occurs when a person has a compulsive need to spend a lot of time on the Internet, to the point of letting other areas of life (such as relationships, study, or health-for example, compared to sleep or nutrition) be affected. Underlying motives involve: elimination of a feeling of discomfort, stress relief, and increased pleasure (Pan, 2020).
- **Hate Speech**- It occurs when offensive speech directed at individuals or groups on the basis of inherent characteristics, such as: ethnicity, religion, gender identity, sexual orientation, and/or disability (Agustinarsih & Yusuf, 2023).
- **Online enticement**- It occurs when someone communicates with a child or adolescent via the Internet with the intent to exploit them. In most cases, there is sexual intent. Online grooming of children occurs in a variety of ways and involves children and adolescents of all ages. It is a broad category of online exploitation that also includes sextortion (see below) (Kasar et al., 2023).

- **Outing and Trickery**- Outing refers to any form of non-consensual disclosure of someone’s information regarding the person; the act of spreading someone's secrets, uncomfortable information, or personal images online; Trickery means pushing a person, through deception, to reveal embarrassing and confidential information about him/herself of another person and then make it public on the Web (Agustiningsih & Yusuf, 2023).



Figure 19. Practical Examples of online conducts that may constitute offenses by law.

- **Revenge porn**- It refers to any form of spreading of a person's sexual or intimate material in the form of photos, videos, conversations, recordings, etc. This form of psychological and sexual violence is often characterized by a pre-existing relationship between the victim and the perpetrator. The materials can be used to blackmail, exploit and/or keep the other person in a role of subordination (Gattamelata, 2022).

- **Sextortion/sex-extortion**- It is a type of exploitation in which a child is induced to take sexually explicit images and/or meet face-to-face with someone for sexual purposes, or engage in an online sexual conversation or, in some cases, sell/trade the child's sexual images. Another risk factor is the act of being threatened to release private or sexual images or videos of the victim unless certain demands are met (O’Malley & Holt, 2022; Gattamelata, 2023).

These phenomena may seem abstract or far from your daily life and direct experience of your kids and students, but in fact many common situations happening everyday may represent criminal offenses for the law. Kids but also adults should be aware that some online conducts are not only wrong and unfair but also illegal. This is important to act in a more conscious

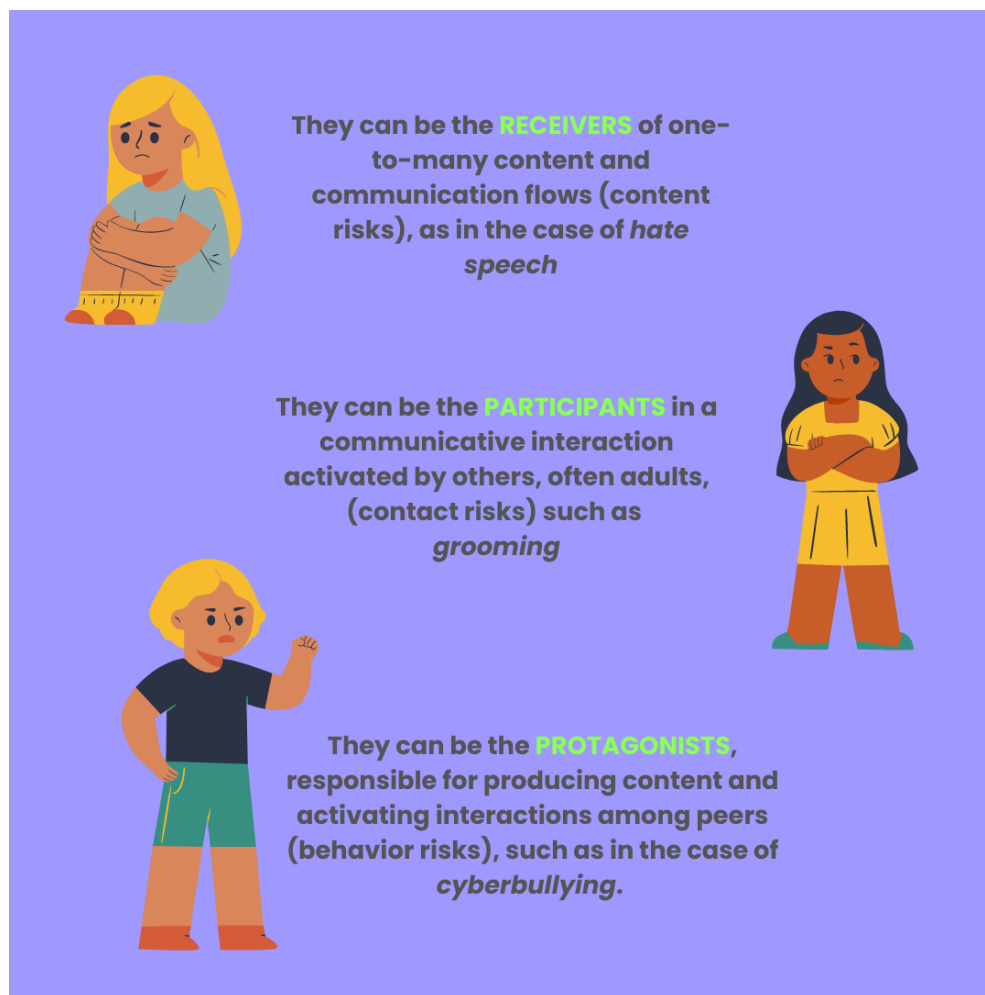


Figure 20. Digital threats and different positions.

way but also to know how to react if being a victim or to support a victim. In Figure 19 you may see some examples of scenarios which could happen to kids online (Bonucchi, & Torretta, 2017).

Negative consequences on development and well-being

From the analyses conducted by **EU Kids Online**, we can find that almost all young people use the Internet on a daily basis for various purposes. In addition, the age of children who have full access to the Internet has also, over the years, gradually decreased (according to some data, about half of 9-10 years old have access). Referring to the potential threats illustrated in this Chapter, young people could find themselves in three different possible positions: receivers, participants and protagonists (see Figure 20).

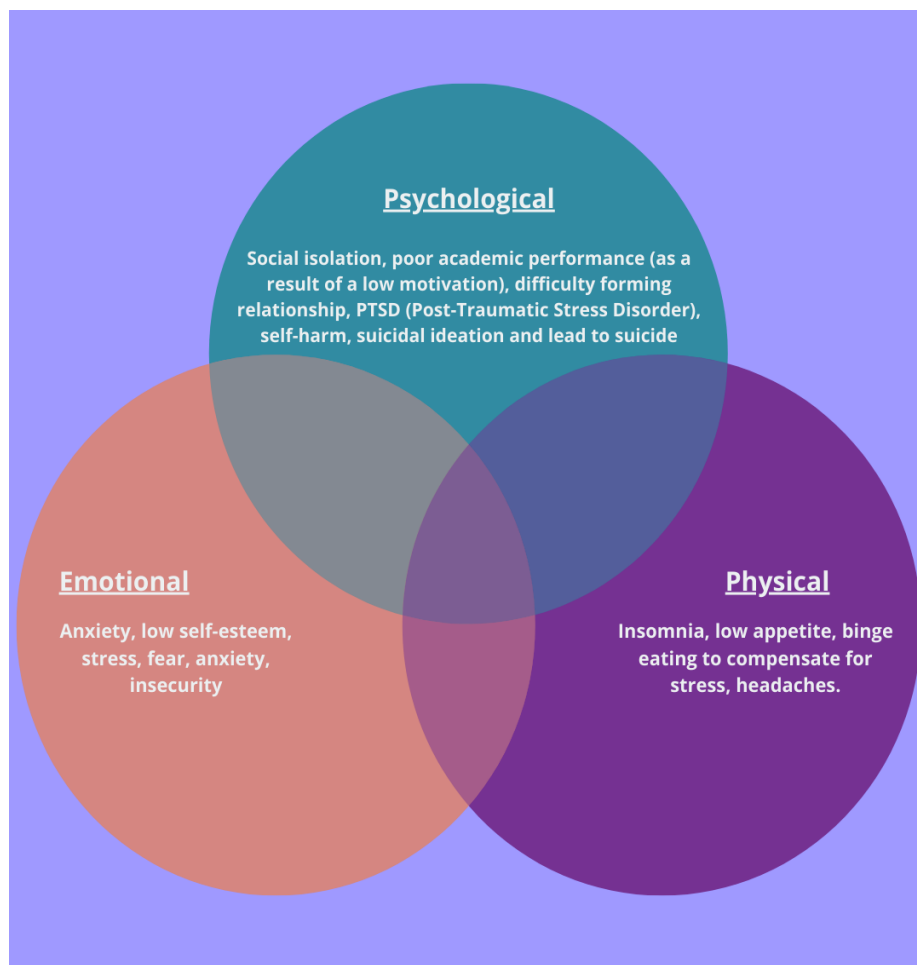


Figure 21. Digital threats and their consequences on children.

It is worth also considering that with respect to some phenomena (e.g., cyberbullying, exclusion) it is not the single exposure that causes harm, but the **repetitiveness** of the episodes. In terms of **negative outcomes** that can occur as a result of the repetitiveness of negative episodes, we can divide them into three aspects, as shown in Figure 21.

These two elements - on one hand, the position of the child or adolescent (Figure 20), on the other hand, the negative effects on health and well-being - relate to each other, generating combinations where the child or adolescent can directly or indirectly experience such negative outcomes (see Figure 21).

Using the internet responsibly: tips for parents, teachers, and children

Being able to communicate online safely for oneself and others is an indispensable asset to a person's well-being in relation to the Internet. To this end, it is important to know some precautions and good practices that, as parents and teachers, it is helpful to discuss with children and students. In addition, to promote healthy listening and effective discussion with them, it is possible to take into account

certain behaviors and tips that the parent or teacher can adopt with their child, student or class group.



Figure 22. 10 Tips for good online interactions.

Netiquette: recommendations for a conscious use of the internet

In the world of the Internet, there are some explicit and implicit rules that it would be best to know to facilitate online communication and relationships. Some of these may seem more obvious, but it is important to understand why they are important; others, however, are not so obvious, so we are going to discover them together. The term "**netiquette**"- derived from the combination of the words "*network*" and "*etiquette*"- refers to the set of rules and behaviors to be adopted for respectful and appropriate communication on the Internet, as well as behavior to prevent any negative outcomes (including legal consequences, penalties and sanctions, considering that some action online are actually crime for the law) (Scheuermann & Taylor, 1997; Al-Khatib, 2023). Here **ten rules of netiquette** we propose you to follow and to pass on to kids at home or at school, for an appropriate behavior online (see Figure 22)

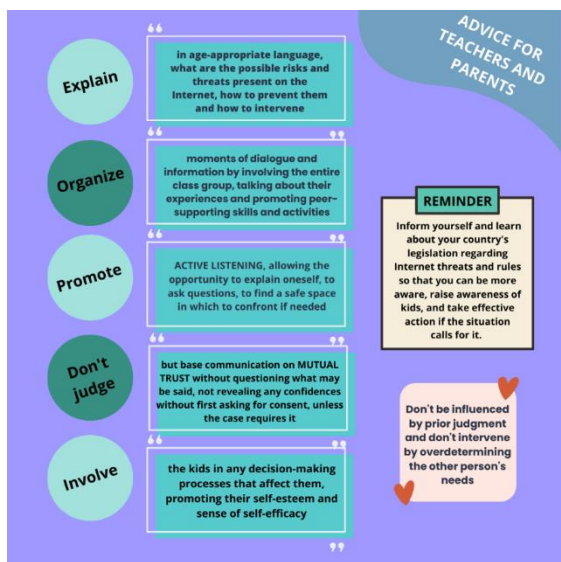
1. **Think that we are and communicate with people, not computers.** Even if one uses technological devices, it is essential to keep in mind that there are people "on the other side." Any offenses, taunts, threats, and insults are not directed at a computer or smartphone, but at one or more people. Often, precisely because of the anonymity that can be used on the Internet (e.g., nicknames, lack of reference to real identity), the inhibition threshold is lowered and, as a result, these harmful behaviors can occur. Unlike face-to-face conversations, moreover, our messages leave traces (e.g., through screenshots), although they can later be deleted. Forgetting about this can lead to denigration and hate speech which beside being wrong and very bad for the emotional sphere of the victim, may constitute crime in some countries.

2. **Respect the others' privacy.** When wanting to share or forward a message, audio, video, or any other material that we have in possession but concerns other people, a person must first ask for their consent. This also applies, for example, to uploading personal photos or videos in the presence of other people, as well as tagging (using their personal social profiles). It must always be clear that this is within cyberspace and that, as mentioned above, much information can remain on the Internet even after it has been deleted. Violation of privacy can constitute a crime and outing, or trickery can be very harmful for victims.
3. **Don't give out your personal information.** Careful attention should be paid to the type of information about oneself shared on the Internet, such as passwords, sensitive data (such as phone number, home address, school name, places frequented, etc.) Whenever possible, it is recommended to use nicknames that are neutral and avoid sharing sensitive information, such as age or personal images to prevent online enticement and other threats related to the exploiting and spreading of personal information without consent.
4. **Don't trust people that you don't know.** It is necessary to approach strangers with a healthy skepticism. One can never know who is really hiding behind the name and photo of a profile. Anyone within an online space could falsify their information (e.g., age of birth) to pursue their own, often malicious, ends. Some people, referred to as "trolls," are individuals who interact for the sole purpose of provoking and irritating with off-topic, nonsensical, and/or outright incorrect messages in order to disrupt the communication itself and torment tempers. In addition, one must be careful about the messages one receives, especially if they come from unknown sources: they may contain attachments that can insert malware that is harmful to our devices and personal information.

5. **Help keep flame wars under control.** Flame wars are messages that contain aggressive personal criticism or attacks on a person. In group chats, heated discussions often degenerate into so-called flame wars. If one finds oneself in such a discussion, they should stay out of it. It should be remembered that insults and threats on the Internet can have legal consequences, beside harming people subject to this.
6. **Don't promote hate speech.** These are often offensive comments under photos or posts. Not infrequently, marginalized social or religious groups e.g., LGBTQIA+ people, foreign or BIPOC people, and people with disabilities, are victims of such actions¹. If one comes across such statements on the Internet, one should report them to the website provider. Providers are obligated by law to delete blatantly illegal content within 24 hours.
7. **Don't abuse your power.** If someone has more power than others within a group, he/she does not have the right to exploit it. For example, preventing people from sending messages in a group chat by blocking them, or changing the rules of a group by overdetermining it just because you are administrator of the group chat is a form of exclusion that can be very detrimental for a person's well-being.
8. **Fairness first: don't exclude anyone.** If one is in a private group, it is best to refrain from making jokes of a personal nature that are not understood by all members of the group: other chat participants should not feel excluded. Also, on the Internet we should all promote values such as tolerance, respect, and helpfulness. This also means that only language used and understood by everyone should be emphasized.

¹ LGBTQIA+ is an abbreviation for “lesbian, gay, bisexual, transgender, queer or questioning, intersex, asexual, and more (+)” and BIPOC is an abbreviation for “Black, Indigenous, and people of color”.

9. **Pay attention to the way you communicate.** Interacting using the language common to all interlocutors (e.g., within a group chat), using correct grammar, spelling, and punctuation, are elements that allow the interlocutor not to be distracted from the goal of the message and make communication effective. It is necessary to know the rules that exist online and use them to the best of advantage to avoid negative experiences; an example of this is the use of caps lock, which communicates that one is yelling or angry. Posts, messages, and questions should be as short and clear as possible. Even the use of items such as stickers (e.g., in group chats) should always be moderate and functional to what you want to communicate.
10. **We don't all have the same timings, and that needs to be taken into account.** Often, because of the speed and immediacy of online communication, it can be expected that others will always be ready and available to respond. It becomes useful, then, to keep in mind that real life timings are different from online times. Another example of how useful it is to respect timing, in a different context, is intervening in a conversation without first carefully reading previous posts. Taking time to understand what circumstance one is in and



whether the question being asked has been answered before shows that one is really interested in the conversation and that one knows how to respect the time another person has taken to respond.

Advice for teachers and parents

By following the rules of netiquette, teachers and parents can support youngsters to avoid incurring certain risks and to understand how they can best communicate in a way that is safe for themselves and others. The ultimate goal is to exploit the Internet to its full potential, safeguarding personal well-being and knowing both its threats and ways to avoid and/or deal with them. It becomes essential, therefore, for those involved in the young person's educational

process, such as parents and teachers, to be aware of this and the ways in which they can foster a healthy process of education and knowledge (Warniasih et al., 2023; Mistretta, 2021). Below you may find some advice for teachers and parents (Figure 23).

Schools, in cases of incidents, should intervene according to *local or school policies* to take disciplinary actions or other measures. In such cases, it is also useful to refer to the expert figures within the school system, such as a psychologist or counselor, to protect the well-being of the student(s) involved.

*“School discipline shall be administered in a manner consistent with the **child’s dignity**. Education should be directed to the development of the child’s personality, talents and abilities, the **respect for human rights and fundamental freedoms**, responsible life in a free society, understanding, tolerance and equality, the development of respect for the natural environment.” Article 28, Convention on the Rights of the Child*

A useful **tool** for parents and teachers is the "**educational contract**," which can be signed between the school and families. This "contract" defines the basis of mutual commitments on which they agree to ensure a good quality of life within school settings. Through the "contract," it is possible to introduce at school the issues related to the use of new media, safe internet surfing, and the risks and threats one may face. This, moreover, indicates that should exist specific norms of behavior within the institution regarding the use of technology, with norms that apply to both students and teachers. It becomes necessary, in these cases, to make explicit what these norms are and why they exist, as well as the consequences one may face in case of transgression.

Conclusions





The pandemic period has been challenging and has accelerated digital transformation in all fields, especially to the field of education. During this period educators, parents and students have overcome a lot of difficulties and learned lessons. Distance learning has really embedded itself into daily teaching practices, through innovative didactic methodologies that promote active learning, peer learning and cooperation. However, teachers and parents should be aware of all the potential benefits and risks, and practices for promoting effective teaching and learning.



The “Data protection and safety in distance learning” STAND Handbook is both theoretical and practical. It provides teachers and parents with theoretical input on different aspects of safety in online learning, while it also includes activities for classroom implementation to raise awareness among primary and secondary school students on the dangers they may encounter when they are online and on the importance of protecting their data and digital identity. Therefore, the STAND team, in the following pages, developed different lesson plans, hoping that this will give teachers, parents and students’ support.

If you have not already done so, we invite you to explore the other project’s resources, the MOOC for teachers’ self-learning (project’s result n.1) and the Methodological Guide for teachers (project’s result n.2) to deepen your knowledge about the use of digital tools.

Classroom Activities

In this section, you may find the activities designed for classroom implementation. The activities are complementary to the content of the Handbook chapters and aim at familiarizing students with some key aspects of online safety and data protection. The partner organizations authored the activities under the supervision of the lead partner of this result - Stimmuli.

Activity	Author	Knowledge & skills	Target Audience
Lesson Plan 1- Sherlock Holmes of Fake news	 STIMMULI for social change	Knowledge on fake news and reliability evaluation, data literacy and research skills.	Primary school pupils (7-12 years old)
Lesson Plan 2- Privacy and GDPR	 BLUE ROOM INNOVATION	Knowledge on legislation data protection, European legislation GDPR.	Secondary school pupils (16-18 years old)
Lesson Plan 3 - Be suspicious.	 DANMAR COMPUTERS IT SOLUTIONS	Knowledge on common cyber threats and potential risks and consequences, skills to protect themselves from cyber threats.	Primary school pupils (6-12 years old)
Lesson Plan 4- Cyber threats awareness	 DANMAR COMPUTERS IT SOLUTIONS	Knowledge on common cyber threats and potential risks and consequences, skills to protect themselves from cyber threats.	Secondary school pupils (12-18 years old)

Lesson Plan 5 – Myself on social media	 <p>STIMMULI for social change</p>	knowledge on digital footprints and identity, collaboration, and research skills	Secondary school pupils (13-18 years old)
Lesson Plan 6 - Let's build together a better internet!	 <p>CENTRO SVILUPPO CREATIVO DANILO DOLCI</p>	knowledge on the risks and threats in the online world, self-reflection, critical thinking and active listening and risk prevention and peer-education skills	Primary and secondary school pupils (8+)

Lesson Plan 1- Sherlock Holmes of Fake news

Educational Level

Primary school

Age of students

6-12 years old

Learning outcomes

By the end of the lesson students will have:

- developed online research skills,
- learned how to spot fake news,
- acquired data literacy skills, and
- learned how to evaluate the reliability of a source.

Time

Preparation time: 2 hours

Teaching time: 45 minutes

Teaching material

Online:

- [Save The Pacific Northwest Tree Octopus \(zapatopi.net\)](#).
- [ppt- Let's break the internet together](#)

Offline:

- LP1 Handout 1: Team name & logo
- LP1 Handout 2: Flowchart
- LP1 Handout 3: SIFT method
- LP1 Handout 4- Evaluation

Lesson Plan

	Procedure	Time
Part 1 Introduction	Divide students in groups of 4-5 based on the number of your class. Tell students that in this class they are going to be detectives like Sherlock Holmes. Then, ask them to find a name for their group, design a logo from on Canva and complete Handout 1: Team name & logo (see Annex).	10 min
Part 2 Theory	Explain the process of finding out whether a website is reliable or not by showing them the presentation (ppt- Let's break the internet together). You will present 2 different ways of identifying reliable resources, SIFT method & flowchart, that is based on SIFT & CRAAP method.	15 min
Part 3 Activity	In this part students act as detectives. Give them the SIFT and the Flowchart handouts. Then, give them access to this website: https://zapatopi.net/treeoctopus Ask them to work together to find out if the website presents reliable information or not. Give them guidelines and answer their questions, if needed.	15 min
Part 4- Debriefing & evaluation	In the end you are going to ask each group about their results. <ul style="list-style-type: none"> ● What did you find out? ● Was it easy to find out if the website had reliable content? ● Were the handouts helpful? ● What was the most challenging/easiest part of the activity? An open discussion follows and collects feedback on the session conducted. Optional: In case there is not enough time left, you can provide students with this quiz (see Annex) to gather feedback on the session.	5 min

Lesson Plan 2- Privacy and GDPR

Educational Level	Age of students
Secondary school	16-18 years old

Learning outcomes

By the end of the lesson students will have:

- developed comprehension and interpretation skills,
- acquired knowledge of legislation regarding data protection and more specifically on the European legislation GDPR,
- learned how to explain terminology related to data protection and data rights.

Time

Preparation time: 3h

Teaching time: 2h

Teaching material

Online:

- Video 1: [GDPR and actors](#)
- Video 2: [A fun video about privacy and person tracking](#)
- Video 3: [Video on GDPR a more complex and complete explanation including rights](#)
- Video 4: [GDPR, actors and principles](#)
- Video 5: [6 principles about GDPR](#)

Offline:

- LP2 Handout 1- Activity 1 Social Networks and Personal Data
- LP2 Handout 2- Activity 1 Social Networks and Personal Data (Questions)
- LP2 Handout 3- Activity 2 Your rights on the internet

Lesson Plan

	Procedure	Time
Part 1 What is GDPR and why	After reading the content of the handbook, explain what the GDPR is and why this law is designed. Then, introduce different key terms and definitions. You can use video 2 and 4 here.	30 min

Part 2 Activity 1 - Discussion	Start Activity 1 “Social Networks and Personal Data” to discuss social media and privacy (Annex: LP2 Handout 1 & 2).	25 min
Part 3 Rights and obligations	After reading the content of the handbook, explain what user rights and obligations are.	30 min
Part 4 Activity 2- Discussion	Start Activity 2 “Your rights on the internet”. Ask your students to reflect on how cookies and privacy settings are used in different websites. You can use this website https://www.decathlon.co.uk/ to initiate discussion (Annex: LP 2 Handout 3)	25 min
Part 4 Debriefing & evaluation	Write or place on a board or wall three faces: smile 😊, indifferent 😐 and sad ☹️. All the students should have some post-its and write in a short sentence how the lesson was. Give them 5 minutes to write their answer. Use the last 5 minutes to summarize the answers and conclude the class.	10 min

Lesson Plan 3 - Be suspicious.

Educational Level

Primary

Age of students

6-12 years old

Learning outcomes

By the end of the lesson students will have:

- defined and identified common cyber threats,
- understood the potential risks and consequences associated with cyber threats,
- developed strategies to protect themselves from cyber threats.

Time

Preparation time: 2h

Teaching time: 45 min.

Teaching material

Online:

- [Cyber security video](#)
- [Cyber security presentation](#)

Offline:

- LP3 and LP4 Handout 1- Activity 1 What type of superhero are you?
- LP3 Handout 2- Activity 2 Online situations
- LP3 Handout 3- Activity 2 Online situations (evaluation)

Lesson Plan

	Procedure	Time
Part 1 Superhero Activity	Teacher gives students Handout 1- Activity 1 What type of superhero are you? Then, students answer the questions and the teacher explains that this is how he got their confidential data and can hack their ICT devices. A discussion follows on the use of the Internet by the students.	5 min
Part 2 Cyber security Definition	Teacher writes on the board CYBER SECURITY and encourages students to think about what it means. Students and teachers work together to create the definition of CYBER SECURITY and discuss how important it is when using ICT devices.	10 min
Part 3 Common cyber threats and safety measures	Teacher shows students the Cyber security video explaining the basics of cyber security. After watching the video students and teacher discuss the questions: 1. What are the dangers of using the internet? 2. Have you ever encountered such threats? If yes, where? 3. How can these treats affect us? What can be the consequences? Teacher introduces some strategies to protect against cyber threats (Cyber security presentation) and explains them briefly. Then he/she divides students into 3 groups (depends on the number of students), their task is to prepare a poster with cyber safety measures. Teacher allows each group to present their poster to the class, fostering peer learning and engagement (with the youngest students the teacher can help kids to prepare one poster).	25 min
Part 4- Evaluation	Teacher puts a happy and a sad face (LP3 and LP4 Handout 3- Activity 2 Online situations (evaluation)) on the floor. The teacher reads the online situations (LP3 Handout 2- Activity 2 Online situations) and students need to decide if they agree or not by standing next to the happy or sad face.	5 min

Lesson Plan 4- Cyber threats awareness

Educational Level

secondary school

Age of students

12-18 years old

Learning outcomes

By the end of the lesson students will have:

- defined and identified common cyber threats,
- understood the potential risks and consequences associated with cyber threats, and
- developed strategies to protect themselves from cyber threats.

Time

Preparation time: 2h

Teaching time: 45 min

Teaching material

Online:

- YouTube videos: [Phishing](#), [Malware](#), [Data breach](#)
- [Cyber security presentation](#)

Offline:

- LP3 and LP4 Handout 1- Activity 1 What type of superhero are you?
- LP4 Handout 2- Activity 2 Comic Strip Template

Lesson Plan

	Procedure	Time
Part 1 -	Teacher gives students handouts with a Superhero questionnaire (Handout 1- Activity 1 What type of superhero are you?), they answer the questions. After completing the task, the teacher explains that this is how he got their confidential data and can hack their social media.	5 min
Part 2	Teacher writes on the board CYBER SECURITY and encourages students to think about what it means. Students and teachers work together to create the definition of CYBER SECURITY and discuss how important it is when using ICT devices.	5 min

Part 3 Common cyber threats	Teacher shows students YT videos (Phishing , Malware , Data breach) explaining common cyber security threats: phishing, malware, data breach. After watching the videos students and teacher discuss the questions: 1. Have you ever encountered this threat? If yes, where? 2. How can it affect someone? What can be the consequences? 3. How can you prevent yourself from this cyber threat? Teacher shows a presentation of strategies to protect against cyber threats (Cyber security presentation). Then he/she divides students into groups, their task is to choose one cyber threat and prepare a short comic (Handout 2- Activity 2 Comic Strip Template) demonstrating preventive measures to protect against that particular threat. Teacher allows each group to present their results to the class, fostering peer learning and engagement.	30 min
Part 4- Evaluation	Teacher summarises the key points discussed during the lesson, emphasizing the importance of preventive measures and responsible online behaviour. Students share one new thing they learned about preventing cybersecurity attacks.	5 min

Lesson Plan 5- Myself on social media

Educational Level	Student's age
Secondary School	13-18 years old

Learning outcomes

By the end of the lesson teachers will have:

- developed research skills,
- acquired knowledge of digital footprints and ways to be protected,
- learned how to protect their digital identity, and
- learn to cooperate and work in teams.

Time

Preparation time: 20 minutes

Teaching time: 45 minutes

Teaching material

Online:

- [Video-Footprints](#)
- [Digital ID and digital footprints presentation](#)

Offline:

- LP5 Handout 1- Activity 1 Do you know that person?
- [LP5 Handout 2- Activity 1 Evaluation](#)

Lesson Plan

	Procedure	Time
Part 1 Discussion	The lesson starts with a short discussion. Ask your students if they use Instagram or other social media like Snapchat or TikTok. After that tell them a story. "Imagine that you post a picture on your social media e.g., Instagram and a friend from your preschool is following you. You haven't seen each other for years, but your friend sees your story. How will it make you feel if that friend shows your story to another friend of yours that is not following you? Or what if that friend takes a screenshot of your story? Or have you ever thought about what you post on the stories? Is it your true self?"	5-7 min

Part 2 Pre-activity	After that short discussion you can show them the following video: Video for digital footprints . After that make clear to them that whatever they post on social media and online in general is permanent and never goes away. Then make a quick presentation on how your digital ID leaves a footprint behind (Digital ID and digital footprints presentation).	15 min
Part 3 Main Activity	Ask your students to split into teams and provide them with the Digital IdentityWorksheet (Handout 1- Activity 1 Do you know that person?). First, you present the structure and content of the worksheet, and you ask them to answer the questions about a person that everyone knows (e.g., a teacher, or school staff). After a while, you ask them to make a Google search about the same person and they fill in the remaining gaps in the worksheet. A discussion follows on Digital Identity among students. What did you learn about this person by this online search?	20 min
Part 4 Evaluation	In the end students evaluate what they learned during the lesson (LP5 Handout 2- Activity 1 Evaluation).	5 min

Lesson Plan 6 - Let's build together a better internet!

Educational Level

Primary school to High school

Age of students

8+ years old

Learning outcomes

By the end of the lesson students will have:

- developed self-reflection, critical thinking, and active listening skills,
- gained knowledge about the risks and threats present in the online world,
- developed risk prevention and peer-education skills.

Time

Preparation time: 30 min

Teaching time: 60+60 min

Teaching material

Online:

- <https://www.mentimeter.com/>

Offline

- Computer
- Projector or digital whiteboard
- Slides (optional)

Lesson Plan

	Procedure	Time
Part 1 Introduction	Start with a brief class discussion on students' experiences regarding their use of the internet and social media to open the discussion and introduce the topic, e.g., How much time do you spend on the internet during the day? For what purpose do you stay on the internet the most?	10 min
Part 2 Prior knowledge	Use <i>Mentimeter</i> or another digital tool to create a word cloud, to gain more insight into the knowledge already present within the class group. Ask students, for example: "What risks might a child or teenager experience on the Internet?", and "What consequences may be suffered because of a wrong use of the Internet"?	10 min

<p>Part 3 Discussion</p>	<p>Allow students time to view the word cloud created through their words and comment with them. Regarding the first question, and the first word cloud, you can ask if they are familiar with all the terms and if they have any experience that they relate back to any phenomenon. Regarding the second question and the second word cloud, you can make them reflect about consequences not only at emotional and psychological level (which are often the first ones which come into mind) but also physical and legal ones. According to the age and level of the class group, you can decide to show a presentation with all (of some of) the definitions presented in this Chapter, adding more specific data about country legislation and legal consequences associated to the mentioned cases, to add to the discussion held with the students, more cases and data that have not come out.</p>	<p>30 min</p>
<p>Part 4 Group work</p>	<p>If you have time (you may divide the activity in two days/lessons and do this step on a second moment) you can ask students to work in groups of 3-4 students each, to write down their own decalogue or “manifesto” to make the internet a better place.</p> <p>You may ask: What should a kid be aware of when using the internet? What suggestions and rules should we follow to better communicate on the internet?</p> <p>After 30 minutes of group work, ask each group to present their rules and all together try to create a class decalogue/manifesto to be posted on the wall and presented to other classes.</p>	<p>60 min</p>
<p>Part 5 Evaluation and conclusion</p>	<p>As a final step, make students reflect about what they already knew (or think they know) about the topic, what they have learned and how they feel about the activity held.</p>	<p>10 min</p>

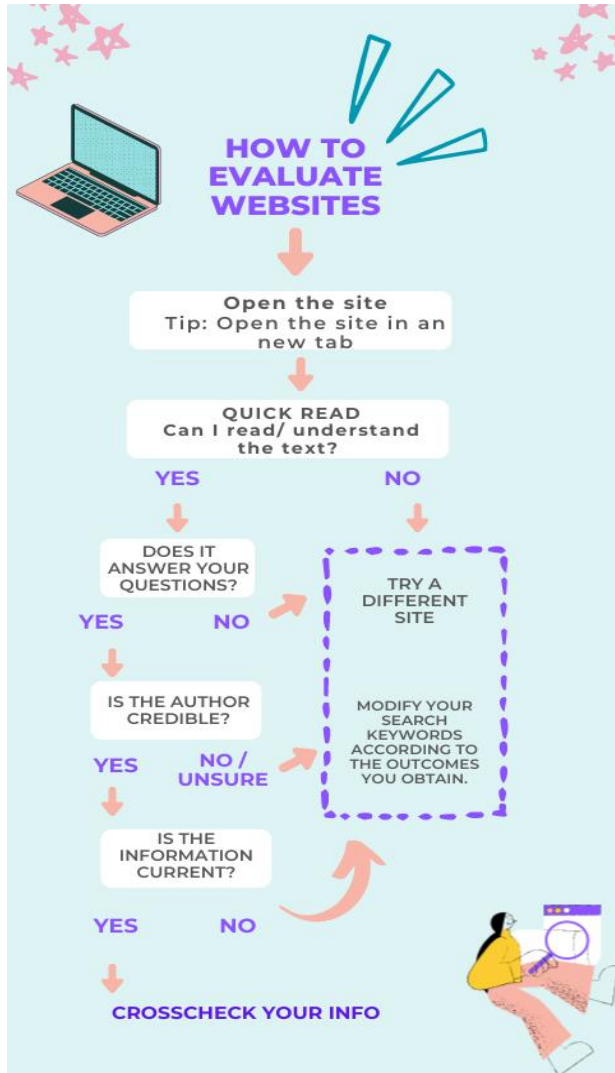
Annex

LP1 Handout 1 – Team name and logo

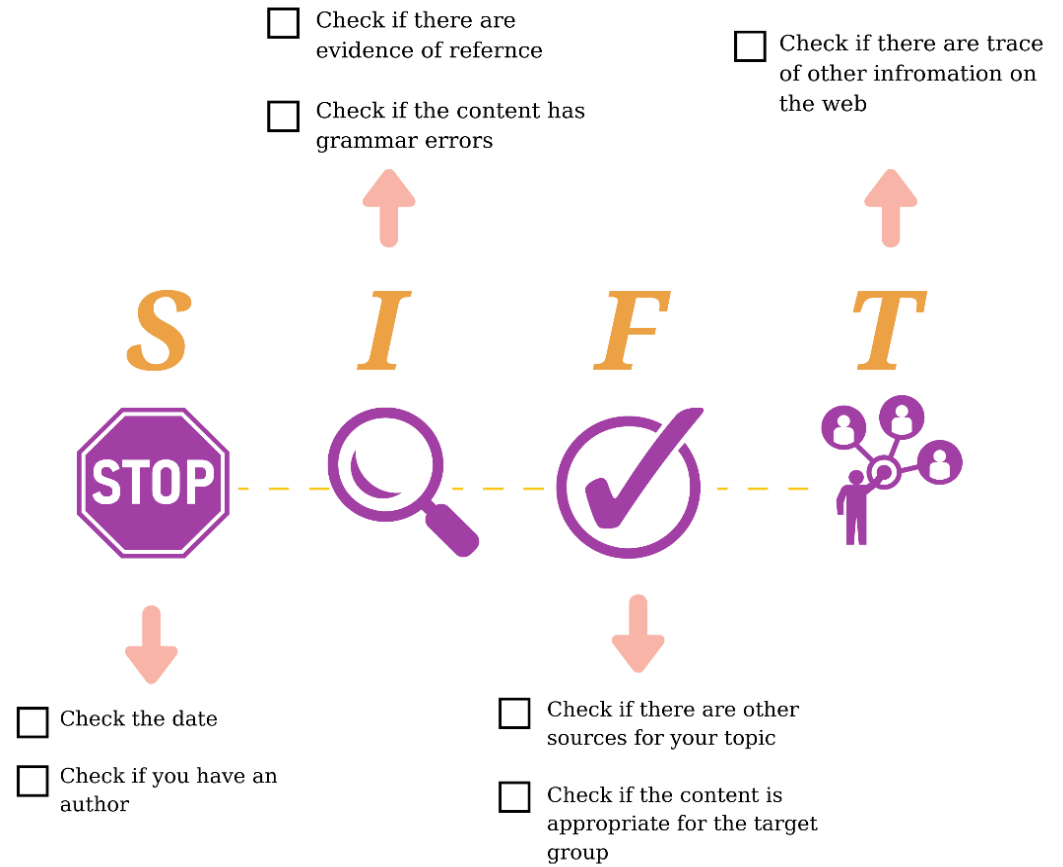
Team's Name:

Logo of the team:

LP1 Handout 2 -Flowchart



Handout 3- SIFT method



LP1 Handout 4- Evaluation


QUIZZZ

Chapter 1- STAND Quiz
4 Questions

NAME : _____

CLASS : _____

DATE : _____

1.  Which method did you try?

A SIFT method B Flowchart Method

2. Did the flowchart or the SIFT method help you?

A Not at all B Yes
 C Absolutely D No

3. Do you believe that you can identify a reliable source on your own?

A I do not know B I am not confident
 C I am confident D I guess

4. Did you like working in teams?

A Yes B No

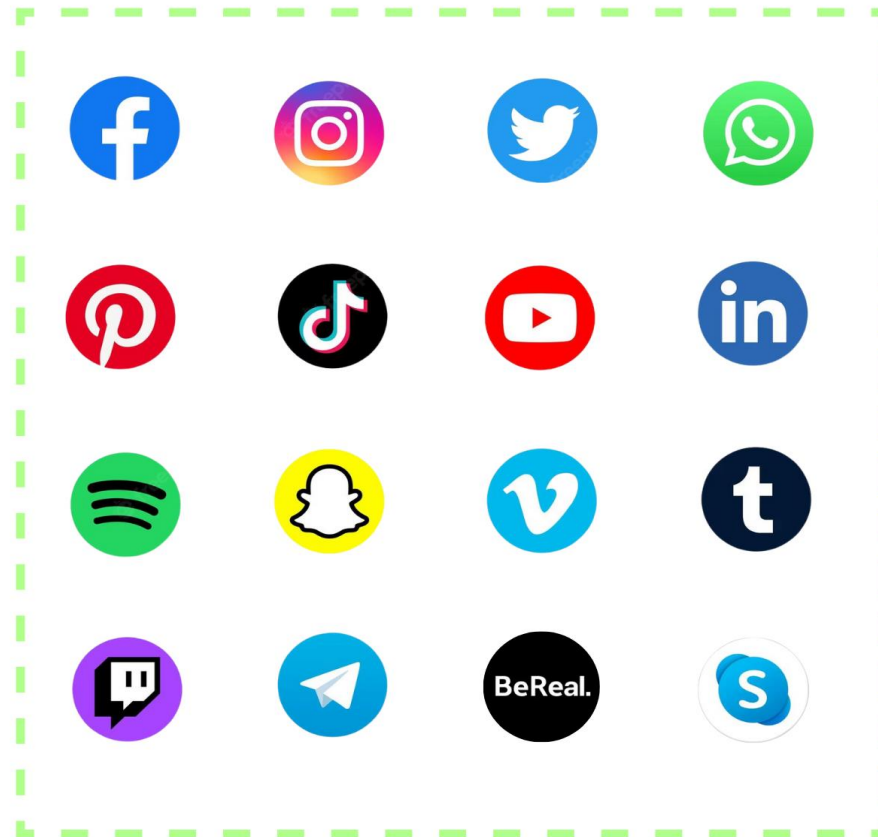
LP2 Handout 1- Activity 1 Social Networks and
Personal Data

ACTIVITY 1



SOCIAL NETWORKS AND PERSONAL DATA

Which 2 do you use the most?



LP2 Handout 2- Activity 1 Social Networks and Personal Data (Questions)

ACTIVITY 1



SOCIAL NETWORKS AND PERSONAL DATA

STEP 1

Start a discussion with students using questions like the following:

1. Ask the class to choose 2 social networks.
2. Reach a consensus as a group on which 2 will be analyzed.

STEP 2

Start a discussion with students using questions like the following:

- What do you use these apps for?
- Which personal data do they ask for?
- Do you have to accept any conditions to gain access?
- Let's analyze some of them together.
- Do you know the age requirements to use different social media apps?
- Did you obtain your parents' permission to sign up for any of these apps?
- Have you ever been asked to enter your date of birth during the sign-up process for apps like these?
- In your opinion, do you think these measures effectively prevent younger children from accessing the platform?

LP2 Handout 3- Activity 2 Your rights on the internet

ACTIVITY 2



YOUR RIGHTS ON THE INTERNET

STEP 1

Choose a website, either the suggested one or any other of your preference.

STEP 2

Start a discussion with students using questions like the following:

- Does the website have a cookie banner?
- Analyze cookie banner. Can you reject cookies? Can you choose cookies preferences?
- Is it easy to access the cookies or privacy explanation on the website?
- Why do you think most cookie policies explain what a cookie is?
- Is it easy to access the privacy policy on the website?
- Read the privacy policy and identify how the website addresses data subject rights.

Note: The website of Decathlon UK serves as a clear example.
<https://www.decathlon.co.uk/>

LP3 and LP4 Handout 1- Activity 1 What type of superhero are you?



What type of superhero are you?

Answer the following questions (with some multiple choice).
Do this as quickly as you can; the first one to submit gets a free superhero sticker pack!

- 1 **How old are you?**
please specify
- 2 **What type of superpower would you prefer?**
 - a) invisibility
 - b) being able to fly
 - c) being ultra-funny
- 3 **What is the name of your street?**
please specify
- 4 **What is the name of your school?**
 - a) Hogwarts
 - b) Rydell High
 - c) another name, please specify
- 5 **What is your favourite flavour of ice cream?**
 - a) chocolate
 - b) vanilla
 - c) strawberry
- 6 **What is your pet's name?**
please specify
- 7 **What is your best friend's name?**
please specify
- 8 **What is your email address?**
please specify

LP3 Handout 2- Activity 2 Online situations

Online situations

Read them to students.
They decide what is OK and what is NOT.



You're online and you meet someone your age in a chat room. You give him or her your address or phone number so you can meet together.

You're online and get a message from the Internet service provider asking for your password. They say they need it to fix your account.

You have downloaded the free game offered by a company.

You got an e-mail from PayNow saying that there was a problem with your account but you ignored it.





LP3 Handout 3- Activity 2 What type of superhero are you? (evaluation)

LP4 Handout 1- Activity 1 Comic Strip Template

COMIC STRIP TEMPLATE

Title: _____

LP5 Handout 1- Activity 1 Do you know that person?

Worksheet- Do you know that person?

Name: _____ Date: _____

What is his/her name?	<input type="text"/>
What is his/ her surname?	<input type="text"/>
Where does he/she live?	<input type="text"/>
What music does she/he listen?	<input type="text"/>
Does he/she have children?	<input type="text"/>
What did he/she study?	<input type="text"/>
What are his/her hobbies?	<input type="text"/>
Which social medi does he/she use more?	<input type="text"/>

LP5 Handout 2- Evaluation

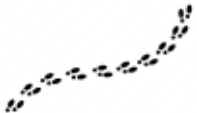
QUIZZZ

digital footprints
4 Questions

NAME : _____

CLASS : _____

DATE : _____

1.  When you make comments on social media, do you leave footprints?

- A I do not know B No
 C It is possible but no D Yes

2.  Which activity makes up a digital footprint?

- A All of them B Post your status
 C Search on the web D Sharing posts online

3. What can you do to make a positive digital footprint for yourself?

- A Post only once a day B Adjust your privacy settings to control who sees your posts
 C Use apps that make pictures and posts disappear like Instagram or Snapchat D Share as much as you can with your best friends

4. How confident do you feel in being able to shape your digital footprint?

- A I am confident B I am not sure
 C I feel extremely confident D I am not confident

References

Agencia Española de Protección de Datos, Autoritat Catalana de Protecció de Dades, Agencia Vasca de References

Agencia Española de Protección de Datos, Autoritat Catalana de Protecció de Dades, Agencia Vasca de Protección de Datos, (2018). *Guía del reglamento general de protección de datos para responsables del tratamiento*. Retrieved from: <https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf>

Agustiningsih, N., & Yusuf, A. (2023). *Types of Cyberbullying Experienced by Adolescents*. Malaysian Journal of Medicine & Health Sciences, 19.

Al-Khatib, T. (2023), *Netiquette rules in online learning through the lens of digital citizenship scale in the post-corona era*. Journal of Information, Communication and Ethics in Society, 21(2).

Arimetrics (2022). Digital Identity, Retrieved from: <https://www.arimetrics.com/en/digital-glossary/digital-identity>

Arkansas State University (2021). Evaluating Websites: Objectivity Retrieved

from: <https://libguides.astate.edu/c.php?g=14517&p=78182#:~:text=Objectivity%20Often%2C%20the%20Internet%20serves%20as%20a%20virtual,presents%20information%20in%20a%20fair%20and%20balanced%20way>

Balaban, D. (2021). How To Protect Your Digital Identity, Forbes, Retrieved from:

<https://www.forbes.com/sites/davidbalaban/2021/09/15/how-to-protect-your-digital-identity/?sh=1a92a6b872c7>

Bonucchi, Torretta, (2017). *Safe Web - seconda parte*. Osservazione e azione per la protezione degli studenti in Rete, Retrieved from:

<https://www.galileivr.edu.it/doc/edusalute/cyberbullismo/SafeWeb2.pdf>

Caulfield, M. (2017), *Web Literacy for Student Fact-Checkers*, PressBooks, Retrieved from: <https://pressbooks.pub/webliteracy/>

- Caulfield, M. (2019). *The SIFT method*, Retrieved from: <https://haggood.us/2019/06/19/sift-the-four-moves/>
- Chen, Y., Conroy, N. J., & Rubin, V. L. (2015). Misleading online content: recognizing clickbait as "false news". In Proceedings of the 2015 ACM on workshop on multimodal deception detection (pp. 15-19).
- Comisión Europea. (2017). Comunicado de La Comisión al Parlamento Europeo y al Consejo. Intercambio y protección de los datos personales en un mundo globalizado. Bruselas. Retrieved from: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017DC0007>
- Colaco, S. (2022). *How Can Educational Institutions Mitigate Cybersecurity Threats in Education?*, Retrieved from: <https://kitaboo.com/how-educational-institutions-mitigate-cybersecurity-threats-in-education/>
- Council of Europe (2019), European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, Handbook on European data protection law – 2018 edition, Publications Office of the European Union, 2019, <https://data.europa.eu/doi/10.2811/343461>
- De Marco, A. (2017). *What Is Sexual Grooming?* Retrieved from: <https://lawofficeofanthonymdemarco.com/sexual-grooming/>
- DeNamur, L.I (2022). *What is a Digital Identity?* Jumio, Retrieved from: <https://www.jumio.com/what-is-a-digital-identity/>
- E. P. (2022). *Agile Phishing – co to jest i jak reagować na oszustwa internetowe?* Retrieved from: https://www.ey.com/pl_pl/consulting/phishing-co-to-jest
- Edwards, C. (2020), *What Is a Digital Identity and How Can You Protect Yours?*, Retrieved from: <https://www.avg.com/en/signal/what-is-a-digital-identity>
- European Commission, (2020). Identifying conspiracy theories, Retrieved from: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/identifying-conspiracy-theories_en

European Parliament (2021). The impact of disinformation on democratic processes and human rights in the world, Brussels, Retrieved from:

[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU\(2021\)653635_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf)

European Parliament (2022a). *EU citizens trust traditional media most, new Eurobarometer survey finds*, Retrieved from:

<https://www.europarl.europa.eu/news/en/press-room/20220704IPR34401/eu-citizens-trust-traditional-media-most-new-eurobarometer-survey-finds>

European Parliament (2022b). Media & News Survey 2022, 2832 / FL011EP, Retrieved from:

<https://europa.eu/eurobarometer/surveys/detail/2832>

European Parliament (2023a). *The influence of social media on the development of children and young people*, Research for Cult Committee,

Retrieved from: [https://www.europarl.europa.eu/RegData/etudes/STUD/2023/733109/IPOL_STU\(2023\)733109_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/733109/IPOL_STU(2023)733109_EN.pdf)

European Parliament (2023b). *Updating the European Digital Identity Framework*, Retrieved from: [Updating the European digital identity](#)

[framework \(europa.eu\)](#)

Gattamelata, A. (2022). Cyberbullismo e revenge porn. *RiCOGNIZIONI. Rivista di Lingue e Letterature straniere e Culture moderne*, 9(18).

GCFGlobal (2023), *What is trolling?*, Retrieved from: <https://edu.gcfglobal.org/en/thenow/what-is-trolling/1/#>

Greek Hoaxes (2020). 53 νεκροί στο Γιβραλτάρ σε 10 ημέρες μετά την έναρξη του εμβολίου της Pfizer, Retrieved from:

<https://www.ellinikahoaxes.gr/2021/01/30/53-dead-gibraltar-pfizer-vaccine-misinformation/>

Gutiérrez, N. (2023). *How to ensure student data privacy: The complete guide*. Retrieved from: [https://preyproject.com/blog/student-data-](https://preyproject.com/blog/student-data-privacy-guide)

[privacy-guide](#)

Harford, I. (2018). *10 common types of malware attacks and how to prevent them*. Retrieved from:

<https://www.techtarget.com/searchsecurity/tip/10-common-types-of-malware-attacks-and-how-to-prevent-them>

IDCentral (2023). *Digital Identity (Digital ID)*, Retrieved from: <https://www.idcentral.io/identity-dictionary/digital-identity-digital-id/>

IFLA (2020). *How to spot fake news*, Retrieved from: <https://repository.ifla.org/bitstream/123456789/1289/2/how-to-spot-fake-news-covid.pdf>

Information Commissioner's Office, (2023). *Individual rights: guidance and resources*. Retrieved from: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/>

Irwin, L. (2018). *The GDPR: When do schools need to report data breaches?* Retrieved from: <https://www.itgovernance.eu/blog/en/the-gdpr-when-do-schools-need-to-report-data-breaches>

ISTE (2015). *Building and Keeping a Positive Digital Identity. A Practical Approach for Educators, Students and Parents*, Retrieved from:

https://uploads.weconnect.com/mce/d5155d043a8e6fffa4385a64df15a176f4752551/school/147-15_ISTE_2015_EdTekWhitepaper_Student_Identity.pdf

Kasar, V., Fernandes, S., Chillarge, A., Abuj, V., & Patil, D. (2023). *Child Predator Detection System On Social Media*, International Journal of Digital Technologies, 2(1)

Kurpiel, S. (2023), *Evaluating Sources: The CRAAP test*, Benedictine University Library, Retrieved from: <https://researchguides.ben.edu/source-evaluation>

Lubeck, Marisa A. (2009). *Satire of News*. Encyclopedia of Journalism. Sterling, C. H. (Ed.), Sage publications

- McCann, M. & Watts, R. (2023), *What Is A VPN Used For?*, Retrieved from: <https://www.forbes.com/advisor/business/software/why-use-a-vpn/>
- Mistretta, S. (2021). *The new netiquette: Choosing civility in an age of online teaching and learning*. International Journal on E-Learning, 20(3), 323-345
- Mubasher, M., Malik, A. S., & Mahmood, A. (2023). *GENDER DIFFERENCES IN EXPERIENCING CYBER-BULLYING AND CYBER-STALKING AMONG YOUNG ADULTS* Masooma Mubasher. Pakistan Journal of Social Research, 5(02), 632-643.
- Munk, V. (2019). When Headlines Amaze, Goethe-Institut Budapest, Retrieved from:
<https://www.goethe.de/ins/hu/de/kul/sup/kl/21485905.html>
- NMU (2018). Evaluating Internet Sources: Authority, Retrieved from: <https://lib.nmu.edu/help/resource-guides/subject-guide/evaluating-internet-sources#tab-337-2>
- Northern Michigan University-NMU (2018). Evaluating Internet Sources, Lydia M. Olson Library, Retrieved from:
<https://lib.nmu.edu/help/resource-guides/subject-guide/evaluating-internet-sources#tab-337-1>
- Nowicka, J., Kopczewski, M., Ciekanski, Z., & Krol, A. (2023). *Cyberspace and Related Threats*, European Research Studies Journal, 26(2), 421-435
- O'Malley, R. L., & Holt, K. M. (2022). *Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime*, Journal of interpersonal violence, 37(1-2), 258-283.
- O'Brien, M. (2021). *How to Protect your School from Malware Attacks*. Retrieved from: <https://www.9ine.com/newsblog/how-to-protect-your-school-from-malware>

Pan, T. (2020). *Psychological and exercise interventions for teenagers with internet addiction disorder*, *Revista Argentina de Clínica Psicológica*, 29(2), 226.

Pan-American Health Organization (2020), *Understanding the infodemic and misinformation in the fight against COVID-19*, DIGITAL TRANSFORMATION TOOLKIT, Retrieved from: https://iris.paho.org/bitstream/handle/10665.2/52052/Factsheet-infodemic_eng.pdf

Rand, H. (2021). *Understanding our digital existence: digital identity versus digital persona*, Retrieved from: <https://www.agrello.io/post/understanding-our-digital-existence-digital-identity-versus-digital-persona>

Scheuermann, L., & Taylor, G. (1997). *Netiquette*. *Internet Research*, 7(4)

SchoolPass (2022). *How schools are using digital IDs to streamline and secure attendance, visitor management, and vaccine tracking*, Retrieved from: <https://schoolpass.com/how-school-use-digital-ids/>

Soni, R. (2023). *Why Identity Management for Education Sector has Become Crucial*, Retrieved from: <https://www.loginradius.com/blog/identity/identity-management-for-education/>

Statista (2023). *Fake news in Europe- statistics & facts*, Retrieved from: <https://www.statista.com/topics/5833/fake-news-in-europe/#topicOverview>

UNHCR (2022). *Factsheet 4:Types of Misinformation and Disinformation*, Retrieved from: <https://www.unhcr.org/innovation/wp-content/uploads/2022/02/Factsheet-4.pdf>

Warniasih, K., Wijayanti, P. S., Syahrurah, J. K., & Rianto, R. (2023). *Online microteaching practices: Developing social competency instruments with the concept of Netiquette*, in *AIP Conference Proceedings* (Vol. 2491, No. 1). AIP Publishing.

Watson, A. (2023). *Fake news in Europe-statistics & facts*, Statista, Retrieved from: <https://www.statista.com/topics/5833/fake-news-in-europe/#topicOverview>

World Economic Forum (2018). *Identity in a Digital World A new chapter in the social contract*, Retrieved from: https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

World Health Organization (2022). Infodemic, Retrieved from: https://www.who.int/health-topics/infodemic#tab=tab_1

World Health Organization (2022). Infodemics and misinformation negatively affect people's health behaviours, new WHO review finds, Retrieved from: <https://www.who.int/europe/news/item/01-09-2022-infodemics-and-misinformation-negatively-affect-people-s-health-behaviours--new-who-review-finds>

World Health Organization (2022). Q&A: How to combat the infodemic with digital solutions to reduce health risks during the COVID-19 pandemic and beyond, Retrieved from: <https://www.who.int/europe/news/item/27-06-2022-q-a--how-to-combat-the-infodemic-with-digital-solutions-to-reduce-health-risks-during-the-covid-19-pandemic-and-beyond>

Yemima, C. K. (2023). *The Forms of Cyberbullying Behavior among Teenage Students: A Systematic Literature Review*. Jurnal Bimbingan dan Konseling Terapan, 7(2), 151-160.

Zarocostas, J. (2020). *How to fight an infodemic*. The Lancet, 395(10225), 676, Retrieved from: [https://www.thelancet.com/journals/lancet/article/PIIS0140-6736\(20\)30461-X/fulltext](https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)30461-X/fulltext)

Zurcher, J. D. (2023). Talking to children about pornography, in *Sex Education Research: A Look Between the Sheets*.