IO2A3

e-Privacing Guide for e-Learning & Personal Data

S&P

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.

Project Nº: 2020-1-UK01-KA226-SCH-094506

Revision History

Version	Date	Author	Description	Action	Pages
[..]	DD/MM/YYYY	PARTNER ORGANIZATION	[Creation/Insert/ Delete/Update of the document]	[C/I/D/U]	[No. of pages]
1.0	22/03/2022	S&P	Creation of document	C	31
2.0	28/03/2022	S&P	Update of document	U	51
3.0	31/03/2022	S&P	Update of document	U	53

(*) Action: C = Creation, I = Insert, U = Update, R = Replace, D = Delete

Referenced Documents

ID	Reference		Title
1	2020-1-UK01-KA226-SCH-094506		e-Privacing Proposal
2			

1 Table of Contents

2 Introduction

The outbreak of COVID-9 and the necessary national measures taken to tackle the spread of the virus caused significant disruption to the provision of education, training and mobility opportunities for learners and teachers across the EU. Helping ensure continuity in education, there is a wide range of online learning material and tools that were made available online (EC, 2020). The EU has already prepared a holistic approach over this issue, taking into consideration the outbreak of COVID-19, the “Shaping Europe’s digital future” (DG Connect 2020) and the EU Digital Education Action Plan (EC, 2020a).

Even though this procedure is a long-term priority for EU, the emerged digitalisation of education due to the pandemic, has raised big concerns over privacy issues and the danger of sharing large amounts of personal data online, and so the national data protection authorities examined issues related to several e-learning platforms and the protection of personal data (HDPA, 2020).

One of the main aspects to be considered in order to achieve a high level of student’s personal data protection is the human factor and particularly the training of teachers and educators, and the awareness of the educational community over the privacy issues.

Most educational institutions passed into the digital era in a sudden and short period of time. Restrictive measures to contain the pandemic affected almost 1.6 billion children in 195 countries worldwide who, suddenly, could no use their classrooms. Initially, educational organisations were using online learning platforms just as an auxiliary tool in the educational process. After the outbreak of COVID-19, these organisations were forced to digitalise every aspect of their operation, without proper examination of the effects in the protection of students’ fundamental rights, such as the protection of their personal data. Schools, universities and educational organisations in general have replaced the traditional way of teaching with the use of existing or new e-learning platform. In some cases, teachers have even used Social Media platforms to deliver online courses throughout the pandemic. Zoom’s security scandal (Wakefield, 2020) proved that in some cased the use of online platforms carries risk for the users (teachers and students).

In addition, the digitalisation of every operational aspect in educational institutions, as a consequence of personnel teleworking policies, created a huge amount of personal data that transmitted and stored online. Taking into consideration all the above, there is clear security gap that exists for the protections of individual’s personal data when using online tools for education and training.

Therefore, the e-Privacing project responds directly to the above issues by mapping existing e-learning platform used in Partners’ countries, by proposing best practices to be adopted by schools and educational centres in the field of data protection, by delivering a GDPR roadmap for teachers and by raising awareness in the educational community with the organisation of multiple events and workshops and by creating an online learning platform to be used as an educational tool for teachers and students over data privacy and protection.

The e-Privacing Guide aims to educate teachers, students and educational institutions on the important topics of data privacy, protection of personal data, and legal obligations of individuals as well as of the institution as a whole.

3 e-Privacing manual for Teachers

The manual for teachers is focused on legal obligations, technical considerations and best practices that the e-Privacing Roadmap suggests. The contents of the manual originate from the emerging requirements of distance education and is based upon real-life examples and applications in secondary education.

3.1 What is Personal Data?

Personal data is any information that relates to a person. Some examples are the following:

- a name and surname
- a home address
- an email address such as name.surname@company.com
- an identification card number
- location data (for example the location data function on a mobile phone)
- an Internet Protocol (IP) address
- a cookie ID
- the advertising identifier of your phone
- data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

3.1.1 What is the value of my personal data?

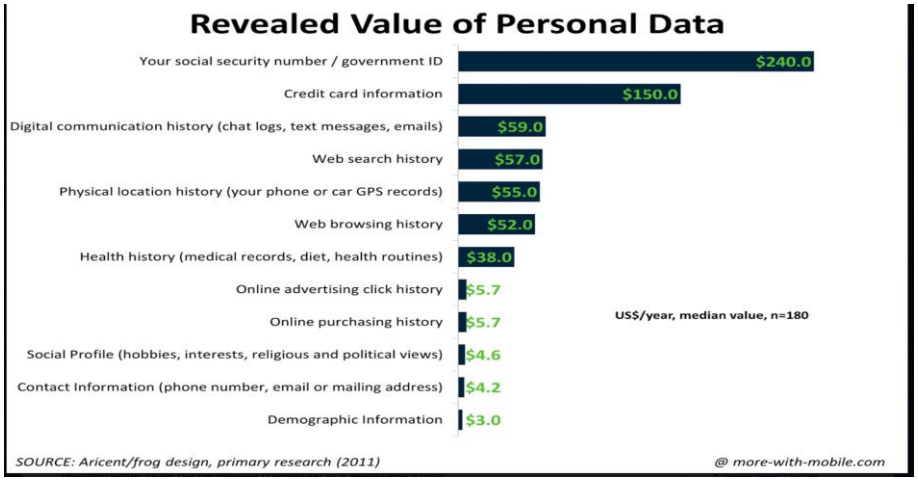


FIGURE 1 VALUE IN US$ OF PERSONAL DATA

3.2 Cookies

Cookies' technology helps the site we visit to remember information about us. Some cookies are important in order the site to operate (necessary cookies), but some cookies are not so innocent. They select information about our online behaviour and our preferences. (e.g., what sites do we prefer to visit, information related to our location and device, as well as information related to preferences).

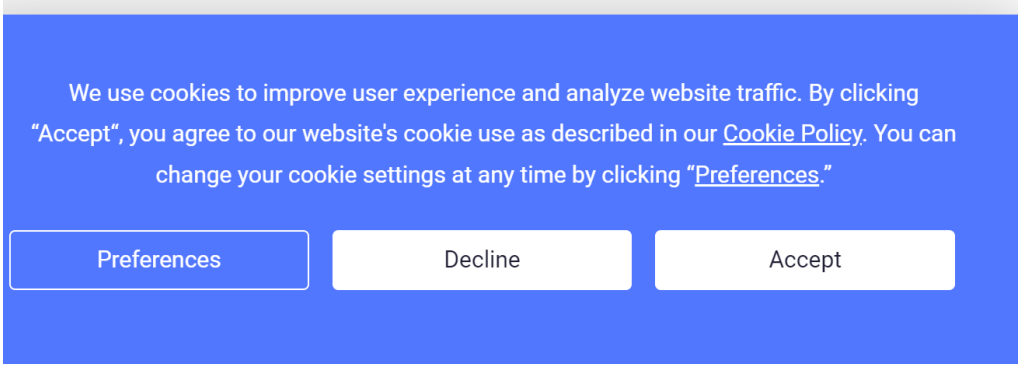


FIGURE 2 DO NOT ACCEPT ALL COOKIES - PROTECT YOUR PRIVACY

3.3 e-Learning Platforms and Privacy

TABLE 1 APPROVED E-LEARNING PLATFORM IN PARTNER COUNTRIES

Country	Platform Name	Link	Education Sector	Login Requirements	Approved by Ministry of Education (Yes/No)
Cyprus	MS Teams	https://www.microsoft.com/el-gr/microsoft-teams/group-chat-software?rtc=1	Public/Private Primary and Secondary	E-mail account and password, two-factor authentication	Yes
Greece	• Webex • eclass	• https://www.webex.com/ • https://eclass.sch.gr/	Public/Private Kindergarten, Primary and Secondary Education	E-mail account and password, access to teachers and students	Yes
Netherlands	Magister	https://www.magister.nl/	Public Primary and Secondary	E-mail account and password, access to teachers, students and parents	Yes
Romania	• Google Meet • Zoom • MS Teams	• https://meet.google.com/landing?authuser=1 • https://zoom.us/ • https://teams.microsoft.com/	Public/Private Kindergarten, Primary/Secondary Education	E-mail account and password, two-factor authentication.	Yes
UK	Glow	https://glowconnect.org.uk/	Public	Being a teacher or education partner in Scotland	Yes

FIGURE 3 ESSENTIAL QUESTIONS TO ASK BEFORE PROVIDING YOUR DATA

3.4 The role of Teachers in the protection of personal data

We should always take into consideration the following:

- Identify which Personal Data of teachers and students are processed by the school.
- Think of my rights as a data subject.
- Think of my obligations as an employee of the school for the process of students' personal data.

3.5 Rights of the Data Subjects

Personal data is any information that relates to an identified or identifiable living individual, and consists of the following rights:

- The Right of Access
- The Right to Information
- The Right to Rectification
- The Right to Erasure
- The Right to Restriction of Processing
- The Right to Data Portability
- The Right to Object
- The Right to Avoid Automated Decision-Making

3.5.1 The Right to Information

- We have the right to be informed about the collection and use of our personal data.
- Information should answer the following questions:
  - Why do you collect my personal data?
  - How long do you keep it?
  - With whom do you share my data?
  - Is it necessary to collect my data for a specific purpose?
- The information provided must be concise, transparent, intelligible, easily accessible, and with the usage of a clear and plain language.

3.5.2 The Right to Access

- We have the right to access and receive a copy of our personal data, and other supplementary information.
- We can make the requests verbally or in writing, including via social media.
- The company/school shall answer within 30 days.
- In case of refusing to implement the request, we have the right to file a complaint to the component data protection authority.

3.5.3 The Right to Rectification

- The right to rectification of personal data is our right to have inaccurate or incomplete personal data.
- We can make the requests verbally or in writing, including via social media.
- In case of refusing to implement the request, we have the right to file a complaint to the component data protection authority.

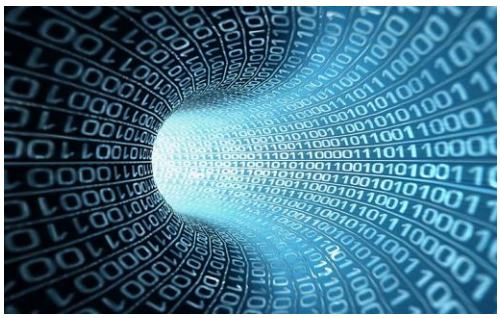
3.5.4 The Right to Erasure ('right to be forgotten')

- We have the right to have personal data erased. This is also known as the 'right to be forgotten'.
- When does the right to erasure apply?
    - The personal data is no longer necessary for the purpose that were collected.
    - Withdrawal of consent.
- In case of refusing to implement the request, we have the right to file a complaint to the component data protection authority.

3.5.5 The Right to Restrict Processing

- We have the right to request the restriction of our data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, it is permitted the storage of the personal data, but not the usage.
- The company/school shall answer within 30 days.
- We can ask the DPO if the right to restrict is applicable.

3.5.6 The Right to Data Portability



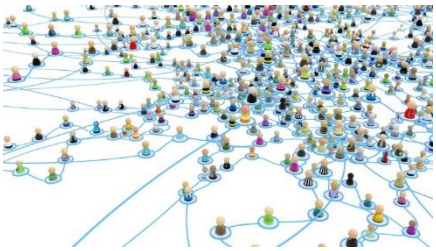
- The right to data portability allows us to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- The company shall answer within 30 days.
- We can ask the DPO for more information.
- In case of refusing to implement the request, we have the right to file a complaint to the component data protection authority.

3.5.7 The Right to Object

- We have the right to object to the processing of our personal data at any time.
- In case of direct marketing, our right is always applicable. This includes any profiling of data that is related to direct marketing.
- This right focuses on the process of our personal data for direct marketing purposes.

That means that we can ask the website to STOP immediately using our personal data for advertising purposes (e.g., personalised ads in social media).

3.5.8 The Right to Avoid Automated Decision-Making



- A significant decision based solely on automated processing cannot be taken.
  e.g., The recruitment procedure
  e.g., The assessment for bank loan
  e.g., The evaluation of students' performance

3.6 Data Breach

A data breach occurs when a cybercriminal successfully infiltrates a data source and extracts sensitive information. This can be done physically by accessing a computer or network to steal local files or by bypassing network security remotely. The latter is often the method used to target companies.

The company shall inform the data subjects as well as the data protection authority.

3.7 Data Protection Officer

We contact the Data Protection Officer in order to:

- Get information about the processing of our personal data
- Get information about the retention period
- Submit a request for the fulfilment of our rights
- Get information about the security measures taken

FIGURE 4 DATA PROTECTION OFFICER (LICENSE- CC BY-ND)

3.8 Which are my choices when my personal data has been violated?

- We can contact the Data Protection Authority in order to get informed about our rights.
- We can lodge a complaint in the Data Protection Authority.
- Under the data protection law, we are entitled to take our case to court to:
    - Enforce our rights under data protection law if we believe they have been breached.

THE OFFICE OF THE Data Protection Authority

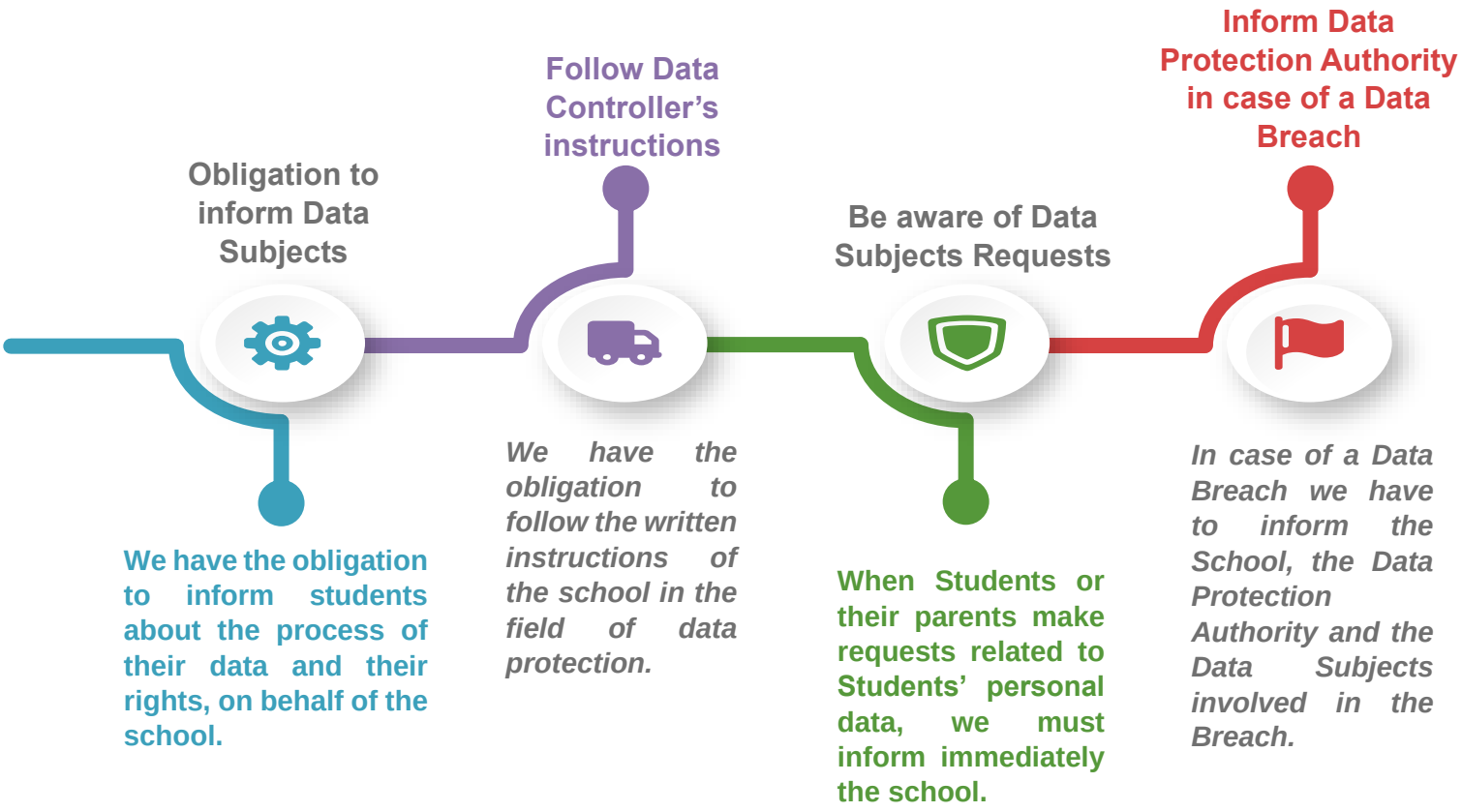
- Claim compensation for any damage caused by any organisation if they have broken data protection law, including any distress we may have suffered.

3.9 Data Protection Authorities in Partner Countries

TABLE 2 CONTACT INFORMATION OF DATA PROTECTION AUTHORITIES IN PARTNER COUNTRIES

Country	Website	E-mail	Telephone
Cyprus	Commissioner for Personal Data Protection	commissioner@dataprotection.gov.cy	+357 22818456
Greece	Αρχή Προστασίας Δεδομένων	contact@dpa.gr	+30 210 6475600
Netherlands	Autoriteit Persoonsgegevens	pers@autoriteitpersoonsgegevens.nl	+31 (0)70 888 85 00
Romania	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal	dpo@dataprotection.ro	+40 318 059 211 +40 318 059 212
UK	https://ico.org.uk/	Scotland@ico.org.uk	+46 0303 123 1113

3.10 Teachers' obligations related to Protection of Personal Data



3.11 Obligations of the Educational Institution

Which are the main obligations of the Educational Institution?

- Conduction of Data Protection Agreements with vendors that process personal data on behalf of the Educational Institution.
- Proper Information to the students and teachers related to the process of their personal data.
- Conduction of Record of Processing Activities.
- Appointment of a Data Protection Officer.
- Conduction of a Data Protection Impact Assessment for the high-risk activities, in order to take special measures for the protection of students' and teachers' personal data.

3.11.1 Data Protection Agreement

An agreement between the educational organisation and the company (vendor) providing the e-learning platform to guarantee the level of protection of the users' personal data. When an educational organisation chooses on of the common e-learning platforms, they should accept specific Terms & Conditions, as well as the Data Protection Agreement.

3.11.2 Proper Information

The Educational organization should provide specific information through its websites' privacy statement to teachers, students, and parents about the processing of their personal data. The privacy statements should consist of specific information about:

- the usage of the e-learning platforms.
- the contact details of the school's Data Protection Officer.
- the way the subjects can exercise their rights.
- the technical and organizational measures taken for the protection of personal data when the students and the teachers use the e-learning platform.

3.11.3 Record of Processing Activities

The educational organisation should keep a record of processing activities and update it with the necessary information related to e-learning platform and online tools they may use. It is recommended to adopt specific data protection policies and procedures over privacy issues.

3.11.4 Data Protection Officer

The educational organisation should appoint a Data Protection Officer to inform the data subjects about specific aspects of the process of personal data, to answer questions and concerns, and to raise awareness about data protection issues as well as to train teachers on the field of privacy and personal data protection.

3.11.5 Data Protection Impact Assessment

The educational should conduct and data protection impact assessment to identify and minimize data protection risks of the usage of e-learning platforms and online tools. In some EU countries, the Data Protection Impact Assessment is conducted by the ministry of education.

3.12 Safe Online Practices and Threats for your Students

3.12.1 Cybersecurity Tips

Staying safe when online decreases the chances of having personal data stolen. The 5 SMART rules when using the Internet in any computer device or mobile phone are presented below:

Safe: Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

Meet: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then, only when they can be present.

Accepting: Accepting emails, IM messages or opening files, pictures or texts from people you don't know, or trust can lead to problems – they may contain viruses or nasty messages.

Reliable: Information you find on the Internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.

Tell: Tell your teacher, parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

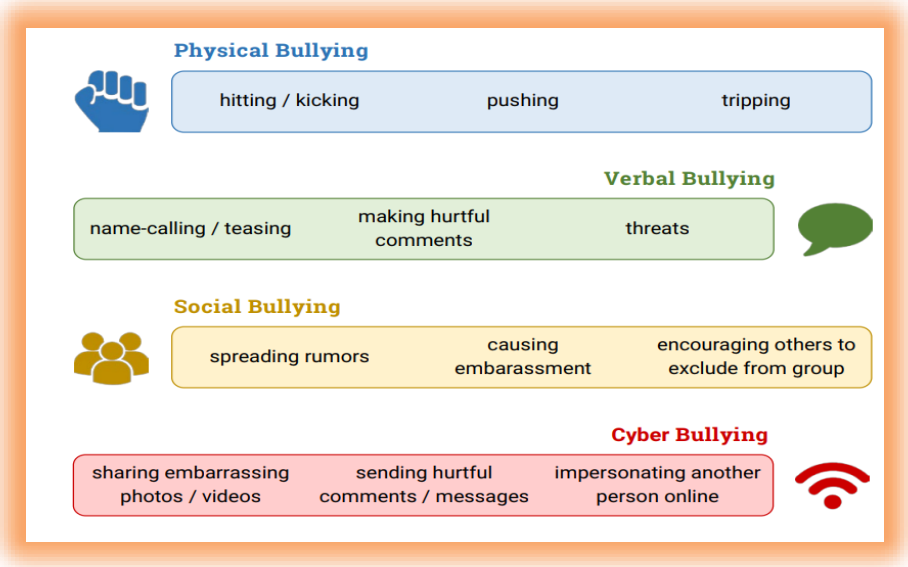
3.12.2 Cyberbullying

What is Bullying and Cyberbullying?

- **Bullying** is purposeful, repeated behaviour designed to cause physical and emotional distress.
- **Cyberbullying** (or online bullying) is bullying using technologies, particularly over the internet or via mobile and gaming networks.
- **Hate speech** attacks a person or group based on their race, religion, sex, sexual orientation, gender identity, and/or physical and mental abilities.

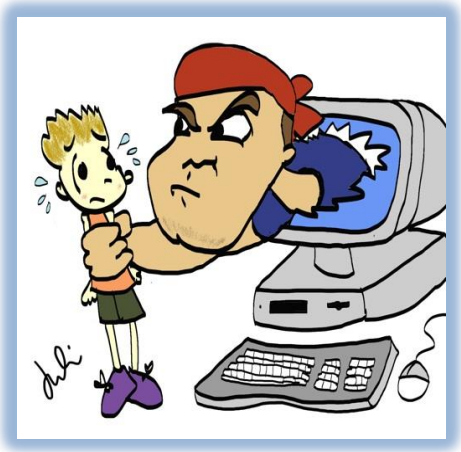
What kind of channels cyberbullies use?

- Social media
- Online gaming communities
- SMS or Text Messages
- Instant Messages (via devices, email provider services, apps, and social media messaging features)
- Phone calls



Technology can be used to carry out a wide range of unacceptable or illegal behaviours such as:

- intimidation and threats
- harassment
- exclusion or peer rejection
- impersonation
- unauthorized publication of personal information or images
- manipulation



Why do people cyberbully?

- Personal, social or family issues
- Early childhood experience, including parenting and maltreatment
- They are taking revenge or may have been bullied themselves
- An acute need for attention, to feel powerful and in control

- Asserting and increasing their popularity and social status
- Poor self-esteem, depression or anger that they cannot manage
- Inability or unwillingness to empathize with others

Consequences of Cyberbullying:

- Loss of self-esteem
- Fear
- Emotional problems (anxiety, stress, sadness, depression)
- Difficulties with schoolwork
- Reluctance to attend school
- Self-harm

Signs that somebody is being cyberbullied (victim):

- Change in mood (sadness, isolation)
- Feeling fearful (Reluctant to go to school or take part in usual social activities)
- Unexplained physical symptoms such as headaches or stomach upsets
- Closing social networking profiles

How can I support a victim of cyberbullying?

- Make it clear that it's not their fault.
- Show them that they are not alone.
- Encourage them to talk to a grown up (parents or teachers that they trust).
- Tell them to take screenshots of the cyberbullying instances to have proof.
- If the bully is your friend, tell him/her is not ok to do this.

Golden rules of Communicating Online

1. **Always respect other people's feelings on the internet.**
2. **Not everyone you meet on the internet is who they pretend to be.**
3. **Never meet someone in person you've only known online.**

If you receive a message that bothers you:

STOP – don't reply to the message but do take a screenshot

BLOCK – block the sender

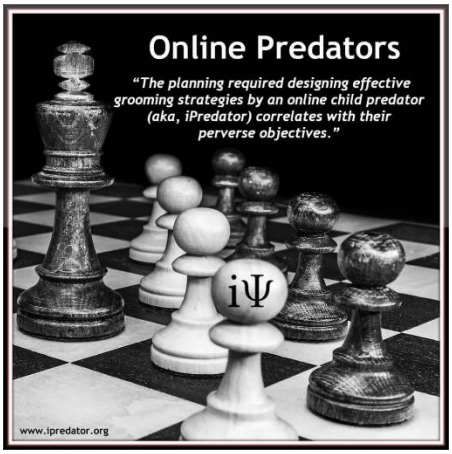
TELL – a trusted adult

3.12.3 Online Grooming

One of the most serious dangers that children may face when browsing online is called online grooming and is when someone, a predator, contacts underage individuals to befriend them and gain their trust in order later to get personal data such as home address, photographs, videos, etc. and extort them in order to get the victim to do things.

Potential consequences:

- Sexual and/or physical abuse
- Embarrassment
- Irritability and anxiety
- Stress and depression
- Substance abuse (drugs, alcohol)
- Long-term emotional damage



Tips for teachers and parents:

- Educate yourselves on relevant national legislation and any helplines you or your students/children can contact.
- Explain to your students/children what online grooming is and what hints they should look for.
- Establish a communication path with your students/children early on so you start building their trust.
- Monitor your students/children internet usage and make sure to check frequently their privacy settings.

3.12.4 Netiquette

Netiquette is a term used to describe responsible, ethical, and polite behaviour while communicating online.

People sometimes forget that although the internet is a new technology that has led to new means of communication, this does not mean that the usual rules and proper ethics of communicating can be dispensed with.

It is important when communicating and interacting online that you act with respect and avoid abusive or bullying behaviour.

Some key principles to bear in mind when online:

<u>Remember the human</u>

It's easy to forget when typing at an inanimate screen that you are communicating with other people who have feelings and experiences you may not be aware of – be respectful

<u>Share carefully</u>

Whatever it is you're posting about, it is important to recall that things can spread unexpectedly quickly online. You can never be sure who has seen or shared your posts!

Stay Vigilant

Just because you see something on the internet, doesn't make it true! Remember to check the veracity of content before you share it. It might be manipulated, taken out of context, or even outright false

Remember your environment

As in the real world, your communication style should change depending on the forum you're in. You should usually be interacting differently with, say, a friend on Facebook than you are with a stranger on Twitter. And don't forget that some sentiments are hard to portray in writing – they can be misunderstood!

3.12.5 Digital Footprint

Everything you do on the internet leaves a digital footprint. Digital footprint refers to the information and data that people generate, through purposive action or passive recording, when they go online (Thatcher, 2014). Your digital footprint is your online reputation.

The Power of Digital Footprints

- All the information online about a person posted either by that person or by others, intentionally or unintentionally.
- Persistent - Lasting a long time. Personal information is stored, accessed, and processed all throughout the web.
- Once something is out on the internet, it can be virtually impossible to erase it.

- If you value your privacy, a digital footprint is your enemy.

There are two main types of digital footprints:

- **Active digital footprints** – these footprints are left actively, examples include social media posts or filling out online forms.
- **Passive digital footprints** – examples include undisclosed cookies or geolocation tools that show your location.

Both types of footprints can be used to track your online activities.

- 70% of employers scan social media profiles of job candidates.
- Having a positive digital footprint is important.

University admissions and employers are increasingly using digital footprints as a means of verifying identity and perceived suitability of candidates for positions within organizations (Benson and Filippaios, 2010).

How to Reduce Your Digital Footprint and Stay Safe Online

- Make sure Wi-Fi connections are secure.
- Make sure you're not sharing too much; be selective about what you share with friends.
- Check privacy setting and adjust them from the default.

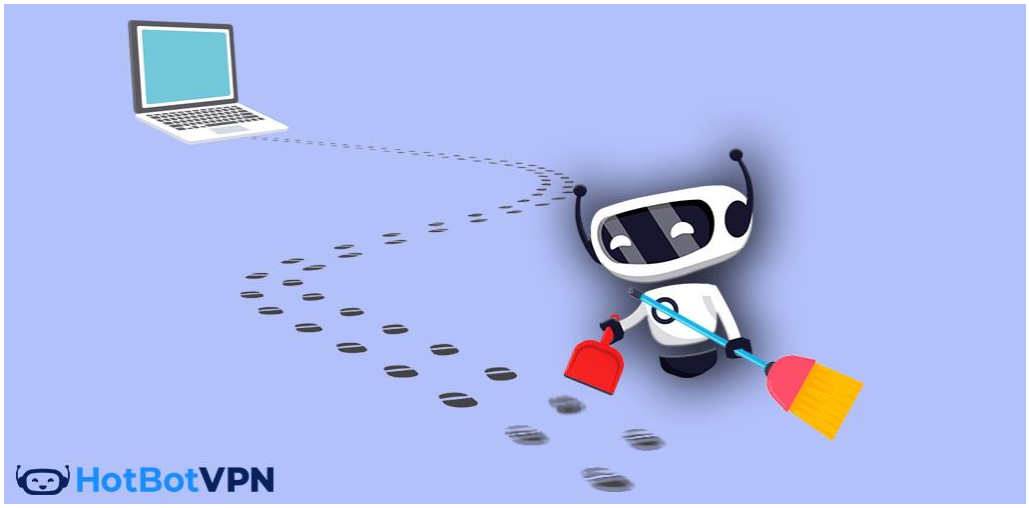


FIGURE 5 SOURCE: HTTPS://WWW.HOTBOT.COM/BLOG/9-STEPS-TO-REDUCE-YOUR-DIGITAL-FOOTPRINT/

How to Leave a Positive Footprint

- **Think before posting**. Always think twice before clicking on links sent in email or through other messaging platforms. If the link has a lot of strange characters in it such as % or $, it is likely a suspicious link and should not be opened.
- Look for **secure web** addresses that begin with https. These are safe and have been encrypted so that no one can steal your information.
- Always remember to **logout** when you are finished online.
- Delete or Deactivate Old Accounts.
- Unsubscribe From Mailing Lists.

Educate your student about their Digital Footprint

- Never share **passwords** with anyone.
- Never share **personal information** such as your name, address, email address, phone number, or what school you attend with people you do not know personally.
- Never share your **location** when online.
- Never share that you are **home alone**.
- Never **guess the URL** of a site you are looking for, use a search engine such as Google to search for the website.
- Never click on sites that **seem questionable,** use information from reputable sites.
- Never **open an attachment** on an email unless you know the sender personally.
- Always **check the sender's email address** to make sure it is a legitimate address.

FIGURE 6 SOURCE: HTTPS://SAFESITTER.ORG/DIGITAL-FOOTPRINTS/

3.12.6 Digital Manipulation

Digital Manipulation can come in various digital forms, such as clickbait, social bots, and fake news. These digital forms of manipulation are designed to influence our opinion and have made their way to our daily activities.

- **Clickbait:** Internet content which encourages the users to follow a link to a webpage by using a catchy headline without sharing any actual or true information.
- **Social bots:** Computer programs that pretend to be real, human users on social media, which sole purpose is to impact online conversations and influence opinions.
- **Fake news:** Fake news is false or misleading information presented as legitimate and accurate news with the aim to damage the reputation of a person or entity or to make money through advertising revenue.

FIGURE 7 'IMAGE: FLATICON.COM'. THIS COVER HAS BEEN DESIGNED USING RESOURCES FROM FLATICON.COM

Some of the dangers of digital manipulation techniques that we need to be aware of:

- Distracting and age-inappropriate content.
- Harmful for a computer device if downloaded (e.g., virus).
- Spread of fake news and misinformation.
- Challenge processes of democratic decision-making.
- Spread racism and conspiracy theories.
- Inflame or suppress social conflict.
- Created to change people's beliefs, attitudes, or perceptions, so they will ultimately change their behaviour.

FIGURE 8 HOW TO SPOT FAKE NEWS

4 e-Privacing manual for Students

The manual is focused on the legal rights and obligations of underage students in regard to the protection of their private data. The contents of the manual originate from the emerging requirements of distance education and will be based on requirements set by the GDPR Framework and National Data Protection Laws.

4.1 What is Personal Data?

Personal data is any information that relates to a person. Some examples are the following:

- a name and surname
- a home address
- an email address such as name.surname@company.com
- an identification card number
- location data (for example the location data function on a mobile phone)
- an Internet Protocol (IP) address
- a cookie ID
- the advertising identifier of your phone

data held by a hospital or doctor, which could be a symbol that uniquely identifies a person.

4.1.1 What is the Value of my Personal Data?

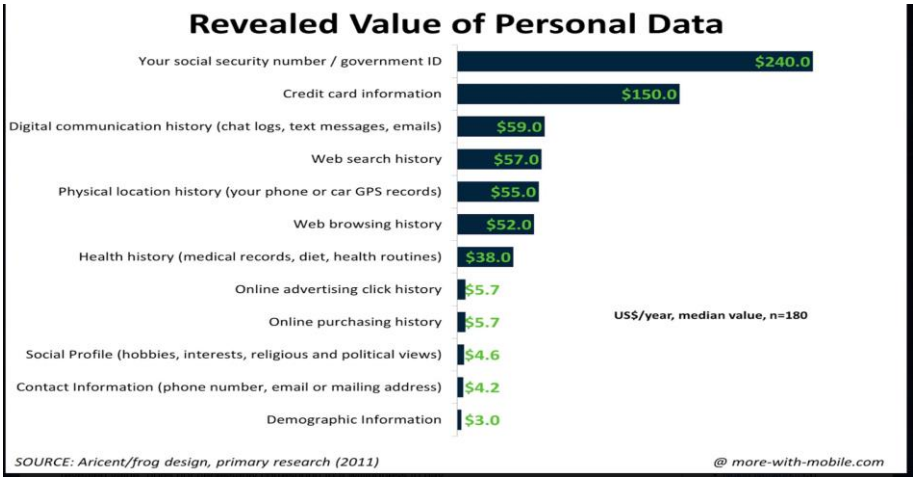


FIGURE 9 VALUE IN US$ OF PERSONAL DATA

4.2 Cookies

Cookies' technology helps the site we visit to remember information about us. Some cookies are important in order the site to operate (necessary cookies), but some cookies are not so innocent. They select information about our online behaviour and our

preferences. (e.g., what sites do we prefer to visit, information related to our location and device, as well as information related to preferences).

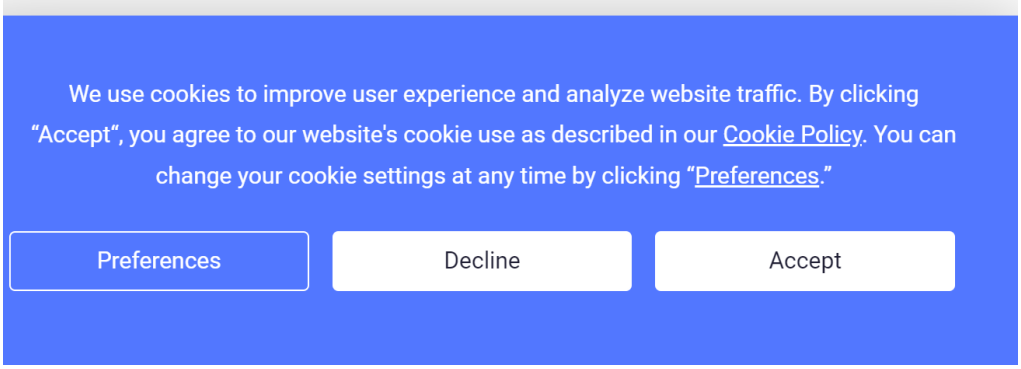


FIGURE 10 DO NOT ACCEPT ALL COOKIES - PROTECT YOUR PRIVACY

4.3 e-Learning Platforms and Privacy

TABLE 3 APPROVED E-LEARNING PLATFORM IN PARTNER COUNTRIES

Country	Platform Name	Link	Education Sector	Login Requirements	Approved by Ministry of Education (Yes/No)
Cyprus	MS Teams	https://www.microsoft.com/el-gr/microsoft-teams/group-chat-software?rtc=1	Public/Private	E-mail account and password, two-factor authentication	Yes
Greece	• Webex • eclass	• https://www.webex.com/ • https://eclass.sch.gr/	Public/Private Kindergarten, Primary and Secondary Education	E-mail account and password, access to teachers and students	Yes
Netherlands	Magister	https://www.magister.nl/	Public	E-mail account and password, access to teachers, students and parents	Yes
Romania	• Google Meet • Zoom MS Teams	• https://meet.google.com/landing?authuser=1 • https://zoom.us/ https://teams.microsoft.com/	Public/Private Kindergarten, Primary/Secondary Education	E-mail account and password, two-factor authentication.	Yes
UK	Glow	https://glowconnect.org.uk/	Public	Being a teacher or education partner in Scotland	Yes

FIGURE 11 ESSENTIAL QUESTIONS TO ASK BEFORE PROVIDING YOUR DATA

4.4 My Rights as a Student

Personal data is any information that relates to an identified or identifiable living individual, and consists of the following rights:

- The Right of Access
- The Right to Information
- The Right to Rectification
- The Right to Erasure
- The Right to Restriction of Processing
- The Right to Data Portability
- The Right to Object
- The Right to Avoid Automated Decision-Making

4.4.1 The Right to Information

- We have the right to be informed about the collection and use of our personal data.
- Information should answer the following questions:
  - Why do you collect my personal data?
  - How long do you keep it?
  - With whom do you share my data?
  - Is it necessary to collect my data for a specific purpose?

The information provided must be concise, transparent, intelligible, easily accessible, and with the usage of a clear and plain language.

4.4.2 The Right to Access

- We have the right to access and receive a copy of our personal data, and other supplementary information.
- We can make the requests verbally or in writing, including via social media.
- The company/school shall answer within 30 days.
- In case of refusing to implement the request, we have the right to file a complaint to the component data protection authority.

4.4.3 The Right to Rectification

- The right to rectification of personal data is our right to have inaccurate or incomplete personal data.
- We can make the requests verbally or in writing, including via social media.
- In case of refusing to implement the request, we have the right to file a complaint to the component data protection authority.

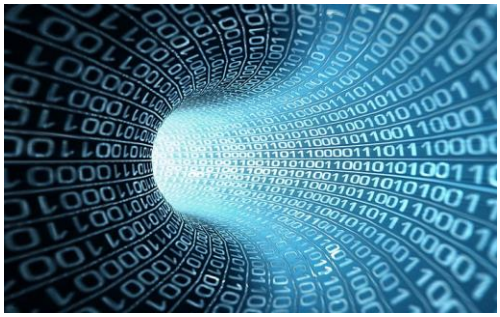
4.4.4 The Right to Erasure ('right to be forgotten')

- We have the right to have personal data erased. This is also known as the 'right to be forgotten'.
- When does the right to erasure apply?
  - The personal data is no longer necessary for the purpose that were collected.
  - Withdrawal of consent.
- In case of refusing to implement the request, we have the right to file a complaint to the component data protection authority.

4.4.5 The Right to Restrict Processing

- We have the right to request the restriction of our data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, it is permitted the storage of the personal data, but not the usage.
- The company/school shall answer within 30 days.
- We can ask the DPO if the right to restrict is applicable.

4.4.6 The Right to Data Portability



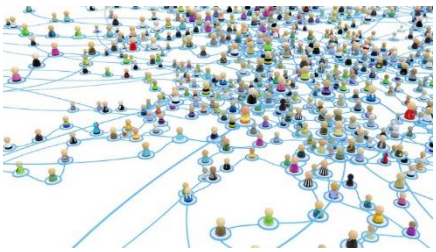
- The right to data portability allows us to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- The company shall answer within 30 days.
- We can ask the DPO for more information.
- In case of refusing to implement the request, we have the right to file a complaint to the component data protection authority.

4.4.7 The Right to Object

- We have the right to object to the processing of our personal data at any time.
- In case of direct marketing, our right is always applicable. This includes any profiling of data that is related to direct marketing.
- This right focuses on the process of our personal data for direct marketing purposes.

That means that we can ask the website to STOP immediately using our personal data for advertising purposes (e.g., personalised ads in social media).

4.4.8 The Right to Avoid Automated Decision-Making



- A significant decision based solely on automated processing cannot be taken.
  e.g., The recruitment procedure
  e.g., The assessment for bank loan
  e.g., The evaluation of students' performance

4.5 Data Breach

A data breach occurs when a cybercriminal successfully infiltrates a data source and extracts sensitive information. This can be done physically by accessing a computer or network to steal local files or by bypassing network security remotely. The latter is often the method used to target companies.

The company shall inform the data subjects as well as the data protection authority.

4.6 Data Protection Officer

We contact the Data Protection Officer in order to:

- Get information about the processing of our personal data
- Get information about the retention period
- Submit a request for the fulfilment of our rights
- Get information about the security measures taken

FIGURE 12 DATA PROTECTION OFFICER (LICENSE- CC BY-ND)

4.7 Which are my choices when my personal data has been violated?

- We can contact the Data Protection Authority in order to get informed about our rights.
- We can lodge a complaint in the Data Protection Authority.
- Under the data protection law, we are entitled to take our case to court to:
    - Enforce our rights under data protection law if we believe they have been breached.

Claim compensation for any damage caused by any organisation if they have broken data protection law, including any distress we may have suffered.

4.8 Contact the Data Protection Authority in your Country

TABLE 4 CONTACT INFORMATION OF DATA PROTECTION AUTHORITIES IN PARTNER COUNTRIES

Country	Website	E-mail	Telephone
Cyprus	Commissioner for Personal Data Protection	commissioner@dataprotection.gov.cy	+357 22818456
Greece	Αρχή Προστασίας Δεδομένων	contact@dpa.gr	+30 210 6475600
Netherlands	Autoriteit Persoonsgegevens	pers@autoriteitpersoonsgegevens.nl	+31 (0)70 888 85 00

Romania	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal	dpo@dataprotection.ro	+40 318 059 211 +40 318 059 212
UK	https://ico.org.uk/	Scotland@ico.org.uk	+46 0303 123 1113

4.9 Obligations of Educational Institution

Which are the main obligations of the Educational Institution?

- Conduction of Data Protection Agreements with vendors that process personal data on behalf of the Educational Institute (e.g., with the company that provides the online platform).
- Proper Information to the students and teachers relating the process of their personal data.
- Conduction of Record of Processing Activities.
- Appointment of a Data Protection Officer.
- Conduction of a Data Protection Impact Assessment for the high-risk activities, in order to take special measures for the protection of students' and teachers' personal data.

4.10 Safe Online Practices and Threats

4.10.1 Cybersecurity Tips

Staying safe when online decreases the chances of having personal data stolen. The 5 SMART rules when using the Internet in any computer device or mobile phone are presented below:

Safe: Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

Meet: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then, only when they can be present.

Accepting: Accepting emails, IM messages or opening files, pictures or texts from people you don't know, or trust can lead to problems – they may contain viruses or nasty messages.

Reliable: Information you find on the Internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.

Tell: Tell your teacher, parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

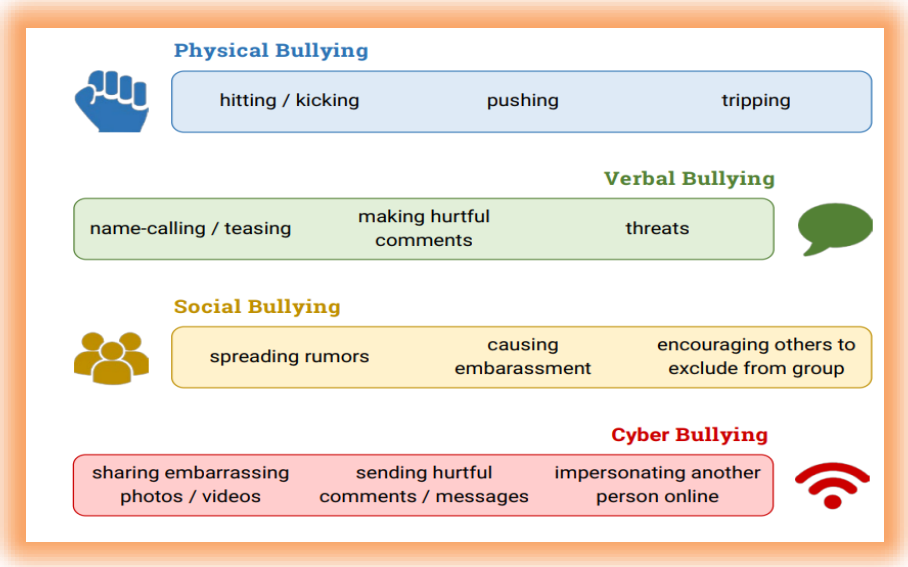
4.10.2 Cyberbullying

What is Bullying and Cyberbullying?

- **Bullying** is purposeful, repeated behaviour designed to cause physical and emotional distress.
- **Cyberbullying** (or online bullying) is bullying using technologies, particularly over the internet or via mobile and gaming networks.
- **Hate speech** attacks a person or group based on their race, religion, sex, sexual orientation, gender identity, and/or physical and mental abilities.

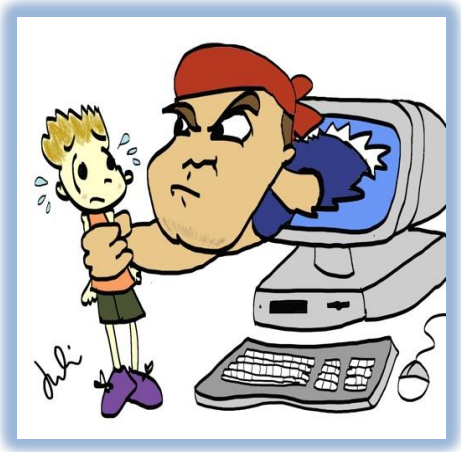
What kind of channels cyberbullies use?

- Social media
- Online gaming communities
- SMS or Text Messages
- Instant Messages (via devices, email provider services, apps, and social media messaging features)
- Phone calls



Technology can be used to carry out a wide range of unacceptable or illegal behaviours such as:

- intimidation and threats
- harassment
- exclusion or peer rejection
- impersonation
- unauthorized publication of personal information or images
- manipulation



Why do people cyberbully?

- Personal, social or family issues
- Early childhood experience, including parenting and maltreatment
- They are taking revenge or may have been bullied themselves
- An acute need for attention, to feel powerful and in control

- Asserting and increasing their popularity and social status
- Poor self-esteem, depression or anger that they cannot manage
- Inability or unwillingness to empathize with others

Consequences of Cyberbullying:

- Loss of self-esteem
- Fear
- Emotional problems (anxiety, stress, sadness, depression)
- Difficulties with schoolwork
- Reluctance to attend school
- Self-harm

Signs that somebody is being cyberbullied (victim):

- Change in mood (sadness, isolation)
- Feeling fearful (Reluctant to go to school or take part in usual social activities)
- Unexplained physical symptoms such as headaches or stomach upsets
- Closing social networking profiles

How can I support a victim of cyberbullying?

- Make it clear that it's not their fault.
- Show them that they are not alone.
- Encourage them to talk to a grown up (parents or teachers that they trust).
- Tell them to take screenshots of the cyberbullying instances to have proof.
- If the bully is your friend, tell him/her is not ok to do this.

How to reduce the risk of Cyberbullying?

- Keep your passwords private.
- Set up privacy controls (only friends can see your information).
- Accept friend requests or follow requests only from people you know.
- Never open messages from people you don't know.
- Think before you post or message something. Any personal information or images can become targets for cyberbullying.

Golden rules of Communicating Online

1. **Always respect other people's feelings on the internet.**
2. **Not everyone you meet on the internet is who they pretend to be.**
3. **Never meet someone in person you've only known online.**

If you receive a message that bothers you:

STOP – don't reply to the message but do take a screenshot

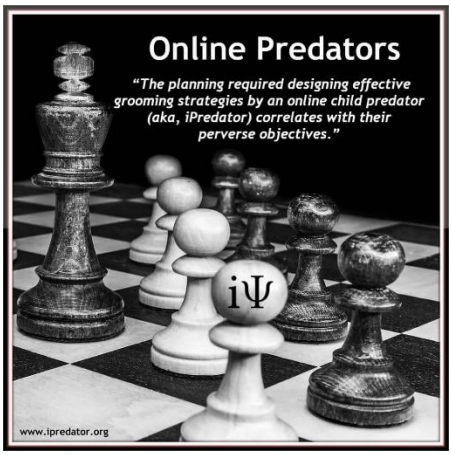
BLOCK – block the sender

TELL – a trusted adult

4.10.3 Online Grooming

One of the most serious dangers that children may face when browsing online is called online grooming and is when someone, a predator, contacts underage individuals to befriend them and gain their trust in order later to get personal data such as home address, photographs, videos, etc. and extort them in order to get the victim to do things.

How to recognize online grooming:



- Their social media profiles have just a few photos of the individual and there are no interactions with other users.
- They offer gifts or rewards without wanting anything back and they make you feel special.
- They ask personal questions and in some cases they start conversations of sexual content, asking photos or videos.
- They ask for personal data, such as school address, phone number and they may ask to meet in secret.

Tips for students:

- You don't have to answer to any stranger you meet online about your personal life and data, such as phone number and address.
- You should ignore such persons and immediately block them.
- You should not accept anything from them, such as presents or gift cards.
- You should ensure you have the correct privacy settings and that your computer device runs the latest security software.
- You must inform immediately an adult that you trust about this issue.

4.10.4 Netiquette

Netiquette is a term used to describe responsible, ethical, and polite behaviour while communicating online.

People sometimes forget that although the internet is a new technology that has led to new means of communication, this does not mean that the usual rules and proper ethics of communicating can be dispensed with.

It is important when communicating and interacting online that you act with respect and avoid abusive or bullying behaviour.

Some key principles to bear in mind when online:

Remember the human

It's easy to forget when typing at an inanimate screen that you are communicating with other people who have feelings and experiences you may not be aware of – be respectful

Share carefully

Whatever it is you're posting about, it is important to recall that things can spread unexpectedly quickly online. You can never be sure who has seen or shared your posts!

Stay Vigilant

Just because you see something on the internet, doesn't make it true! Remember to check the veracity of content before you share it. It might be manipulated, taken out of context, or even outright false

Remember your environment

As in the real world, your communication style should change depending on the forum you're in. You should usually be interacting differently with, say, a friend on Facebook than you are with a stranger on Twitter. And don't forget that some sentiments are hard to portray in writing – they can be misunderstood!

4.10.5 Digital Footprint

Everything you do on the internet leaves a digital footprint. Digital footprint refers to the information and data that people generate, through purposive action or passive recording, when they go online (Thatcher, 2014). Your digital footprint is your online reputation.

The Power of Digital Footprints

- All the information online about a person posted either by that person or by others, intentionally or unintentionally.
- Persistent - Lasting a long time. Personal information is stored, accessed, and processed all throughout the web.
- Once something is out on the internet, it can be virtually impossible to erase it.

- If you value your privacy, a digital footprint is your enemy.

There are two main types of digital footprints:

- **Active digital footprints** – these footprints are left actively, examples include social media posts or filling out online forms.
- **Passive digital footprints** – examples include undisclosed cookies or geolocation tools that show your location.

Both types of footprints can be used to track your online activities.

- 70% of employers scan social media profiles of job candidates.
- Having a positive digital footprint is important.

University admissions and employers are increasingly using digital footprints as a means of verifying identity and perceived suitability of candidates for positions within organizations (Benson and Filippaios, 2010).

How to Reduce Your Digital Footprint and Stay Safe Online

- Make sure Wi-Fi connections are secure.
- Make sure you're not sharing too much; be selective about what you share with friends.
- Check privacy setting and adjust them from the default.

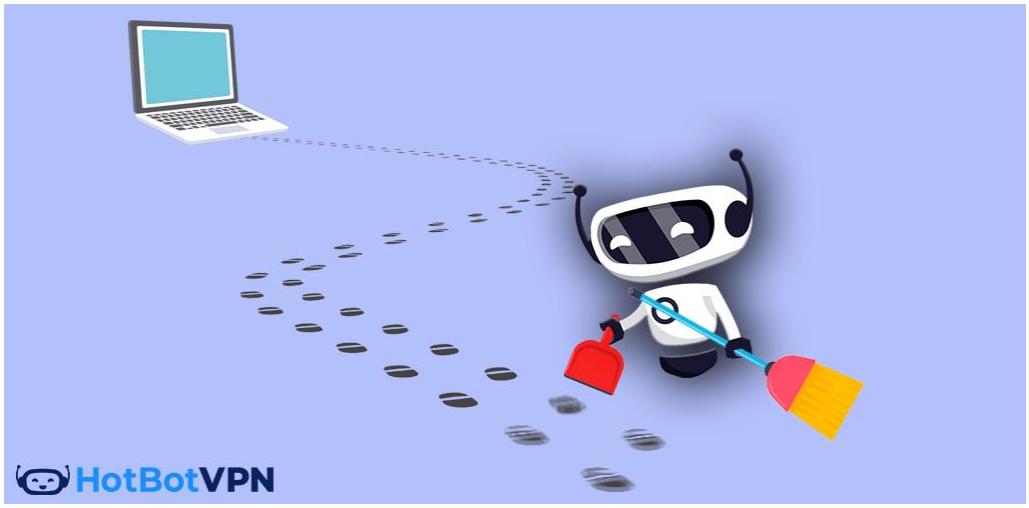


FIGURE 13 SOURCE: HTTPS://WWW.HOTBOT.COM/BLOG/9-STEPS-TO-REDUCE-YOUR-DIGITAL-FOOTPRINT/

How to Leave a Positive Footprint

- **Think before posting**. Always think twice before clicking on links sent in email or through other messaging platforms. If the link has a lot of strange characters in it such as % or $, it is likely a suspicious link and should not be opened.
- Look for **secure web** addresses that begin with https. These are safe and have been encrypted so that no one can steal your information.
- Always remember to **logout** when you are finished online.
- Delete or Deactivate Old Accounts.
- Unsubscribe From Mailing Lists.

Educate your student about their Digital Footprint

- Never share **passwords** with anyone.
- Never share **personal information** such as your name, address, email address, phone number, or what school you attend with people you do not know personally.
- Never share your **location** when online.
- Never share that you are **home alone**.
- Never **guess the URL** of a site you are looking for, use a search engine such as Google to search for the website.
- Never click on sites that **seem questionable,** use information from reputable sites.
- Never **open an attachment** on an email unless you know the sender personally.
- Always **check the sender's email address** to make sure it is a legitimate address.

FIGURE 14 SOURCE: HTTPS://SAFESITTER.ORG/DIGITAL-FOOTPRINTS/

4.10.6 Digital Manipulation

Digital Manipulation can come in various digital forms, such as clickbait, social bots, and fake news. These digital forms of manipulation are designed to influence our opinion and have made their way to our daily activities.

- **Clickbait:** Internet content which encourages the users to follow a link to a webpage by using a catchy headline without sharing any actual or true information.
- **Social bots:** Computer programs that pretend to be real, human users on social media, which sole purpose is to impact online conversations and influence opinions.
- **Fake news:** Fake news is false or misleading information presented as legitimate and accurate news with the aim to damage the reputation of a person or entity or to make money through advertising revenue.

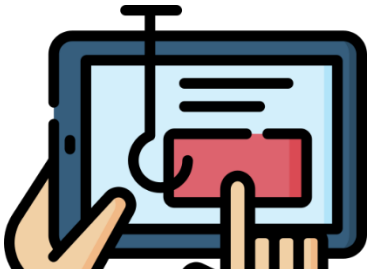


FIGURE 15 'IMAGE: FLATICON.COM'. THIS COVER HAS BEEN DESIGNED USING RESOURCES FROM FLATICON.COM

How to protect against Clickbait, Social bots and Fake news:

- Avoid clicking on posts that contain promotions of “exclusive”, “shocking”, or “sensational” news.

- Hover over a link to check its true destination and avoid unfamiliar websites.
- Ignore public opinions from accounts you're unsure of and do not be easily swayed by content posted on social media.
- Report account/user to the social media platform, that will expedite the removal of the bot.
- Consider the source and the author before believing a post you read.
- Ask and adult or consult a fact-checking website.

FIGURE 16 HOW TO SPOT FAKE NEWS

5 Conclusion

Education systems across Europe faced numerous challenges in the rapid transition to online learning that was necessitated by the onset of the Covid-19 pandemic in terms of the quality and fashion of the learning itself, but also in terms of adapting to digital platforms. Teachers and academic staff had little to no training on e-learning and the adoption of new platforms and new means of teaching altogether brought additional difficulties when it came to digital privacy and data privacy.

Indeed, although there is plenty of literature around the broader switch to digital learning (despite the pandemic being not just extremely recent but also still ongoing) and its challenges, there seems to have been relatively little on the observance and knowledge (or lack thereof) about digital privacy rights and obligations. This seems to have applied as much to students, who for a variety of reasons may be particularly vulnerable in this respect, as it does to teachers and academic institutions.

The e-Privacing Guide covers subjects such as digital privacy and data protection rights specific to education, along with some informative and comprehensive educational content on digital threats. e-Privacing encourages the use of digital means in the educational system of EU countries while suggesting a holistic approach towards the protections of personal data. By creating a roadmap for compliant technological solutions in the field of digital education and by training the users of these platforms to respect the EU privacy legislation and to avoid data breaches, the e-Privacing goal is achieved.

6 References

- Be Internet Citizens. Retrieved from https://internetcitizens.withyoutube.com/
- Buchanan R, Southgate E, Smith SP, Murray T, Noble B. Post no photos, leave no trace: Children's digital footprint management strategies. E-Learning and Digital Media. 2017;14(5):275-290. doi:10.1177/2042753017751711. Retrieved from https://journals.sagepub.com/doi/full/10.1177/2042753017751711
- CareerBuilder (2017), Number of Employers Using Social Media to Screen Candidates at All-Time High, Finds Latest CareerBuilder Study. Retrieved from https://www.prnewswire.com/news-releases/number-of-employers-using-social-media-to-screen-candidates-at-all-time-high-finds-latest-careerbuilder-study-300474228.html
- COMMON SENSE MEDIA (2018), How do I teach my kids about clickbait? Retrieved from https://www.salon.com/2018/11/17/how-do-i-teach-my-kids-about-clickbait_partner/
- Cyber safety guide for middle school kids. Retrieved from https://hk-en.norton.com/internetsecurity-kids-safety-middle-school-kit-a-broader-world-of-cybersecurity-protection.html
- Cyberbullying facts and advice | Internet Matters'. Retrieved from https://www.internetmatters.org/issues/cyberbullying/
- Cyberbullying. Retrieved from https://saferinternet4kids.gr/wp-content/uploads/2017/01/Brochure_Cyberbullying.pdf

- DG Connect (2020), Digital technologies - actions in response to coronavirus pandemic: Skills, collaborative working and creativity. Retrieved from https://ec.europa.eu/digital-single-market/en/content/digital-technologies-actions-response-coronavirus-pandemic-skills-collaborative-working-and
- Directorate-General for Internal Policies (2016), Cyberbullying among young people. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf
- EC (2020), Coronavirus: online learning resources. Retrieved from https://ec.europa.eu/education/resources-and-tools/coronavirus-online-learning-resources_en
- EC (2020a), Digital Education Action Plan (2021-2027). Retrieved from https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
- EC (2021). Digital privacy. The ePrivacy Directive and the General Data Protection Regulation help ensure digital privacy for EU citizens. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/digital-privacy
- Efi A. Nisiforou, Panagiotis Kosmas & Charalambos Vrasidas (2021): Emergency remote teaching during COVID-19 pandemic: lessons learned from Cyprus, Educational Media International, DOI: 10.1080/09523987.2021.1930484
- Gabel, D.; Hickman, T. (2019). GDPR Guide to National Implementation. Retrieved from https://www.whitecase.com/publications/article/gdpr-guide-national-implementation
- Google (2018), Be Internet Legends. Retrieved from https://storage.googleapis.com/gweb-interland.appspot.com/en-gb-all/hub/pdfs/Google_InternetLegends_Curriculum.pdf
- Gracey, L (2017), Teaching kids (and adults) about clickbait, Retrieved from https://blog.tcea.org/clickbait/
- Hall, T., Connolly, C., Ó Grádaigh, S., Burden, K., Kearney, M., Schuck, S., Bottema, J., Cazemier, G., Hustinx, W., Evens, M., Koenraad, T., Makridou, E., & Kosmas, P. (2020). Education in precarious times: A comparative study across six countries to identify design priorities for mobile learning in a pandemic. Information and Learning Sciences, 121(5/6), 433–442. https://doi.org/10.1108/ILS-04-2020-0089
- HDPA (2020), Opinion 4/2020 of the Hellenic Data Protection Authority. Retrieved from https://bit.ly/2SwyVGl
- Kids Helpline (2018), Cyberbullying | How to Protect Yourself & Get Support. Retrieved from https://kidshelpline.com.au/teens/issues/cyberbullying
- Kids Safety (kaspersky.com) (2015), Recognising the Signs of Cyberbullying. Retrieved from https://kids.kaspersky.com/recognising-the-signs-of-cyberbullying/
- Kidshelpline (2019), Understanding online grooming. Retrieved from https://kidshelpline.com.au/parents/issues/understanding-online-grooming
- Nemours KidsHealth (2018), Cyberbullying (for Teens). Retrieved from https://kidshealth.org/en/teens/cyberbullying.html

- OECD. (2020). OECD policy responses to coronavirus (COVID-19): The impact of COVID-19 on student equity and inclusion: Supporting vulnerable students during school closures and school re-openings. Retrieved from https://read.oecd-ilibrary.org/view/?ref=434_434914-59wd7ekj29&title=The-impact-of-COVID-19-on-student-equity-and-inclusion
- Rouse, M (2019), Cybersecurity. Retrieved from https://searchsecurity.techtarget.com/definition/cybersecurity
- Sarang, R. (2018), Back to School: 5 Cybersecurity Habits to Teach Your Kids. Retrieved from https://securingtomorrow.mcafee.com/consumer/mobile-and-iot-security/back-to-school-cybersecurity-habits-for-kids/
- StopBullying.gov (2021), What Is Cyberbullying. Retrieved from https://www.stopbullying.gov/cyberbullying/what-is-it
- UNESCO. (2020). COVID-19 educational disruption and response. Retrieved from https://en.unesco.org/covid19/educationresponse
- Wakefield, J. (2020), Zoom boss apologises for security issues and promises fixes. Retrieved from https://www.bbc.com/news/technology-52133349
- Webwise.ie, Lesson 2: What is Cyber Bullying? Retrieved from https://www.webwise.ie/teachers/myselfielesson2/
- Webwise.ie, Lesson 3 - How bullying feels and how best to respond. Retrieved from https://www.webwise.ie/teachers/myselfielesson3/