2020-1-UK01-KA226-SCH-094506

IO2A1: e-Privacing Manual for Teachers

e-Learning and Personal Data

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

This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Table of Contents (1/2)

Table of Contents (2/2)

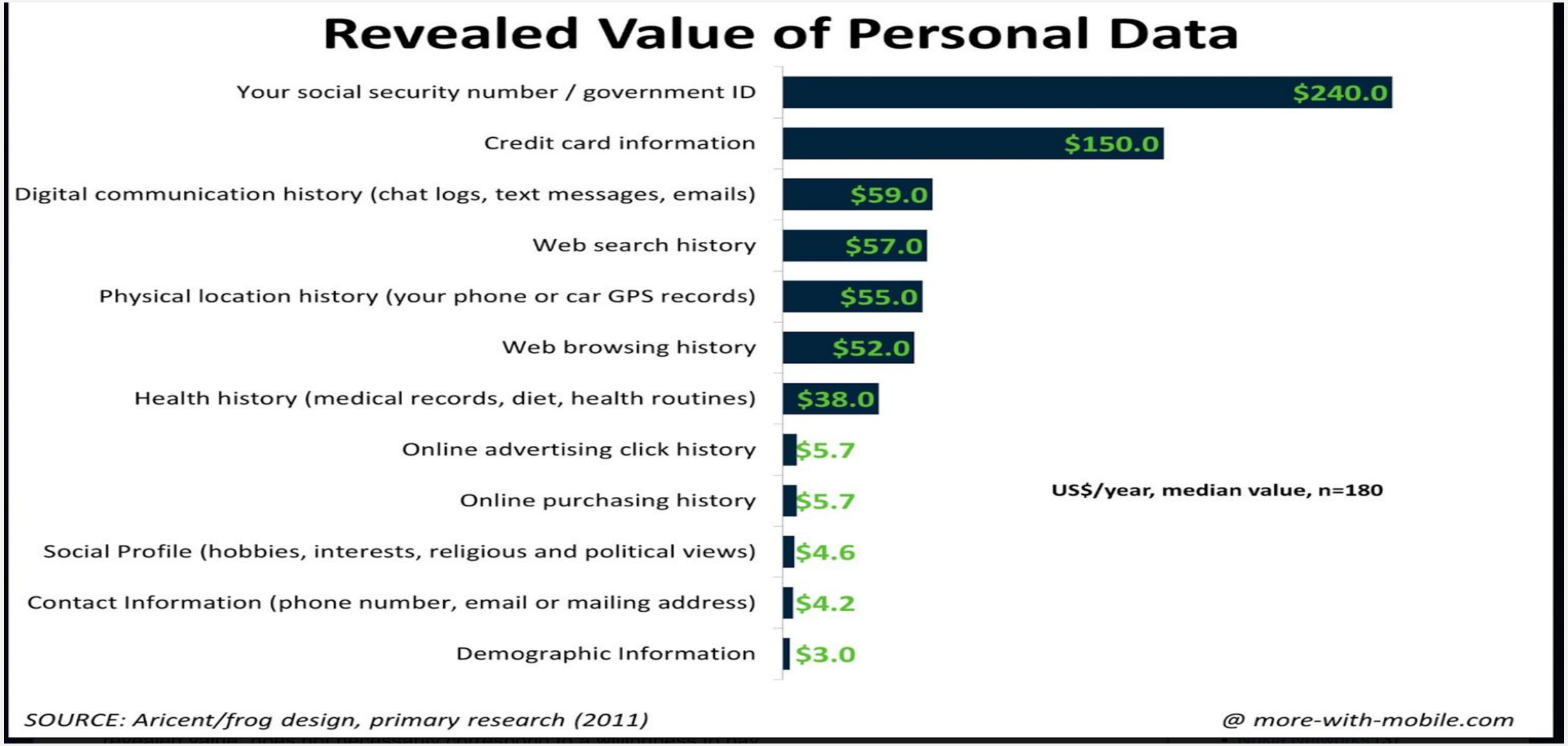
What is Personal Data?

Personal data is any information that relates to a person.

Examples:

- 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.

Which is the value of my Personal Data?



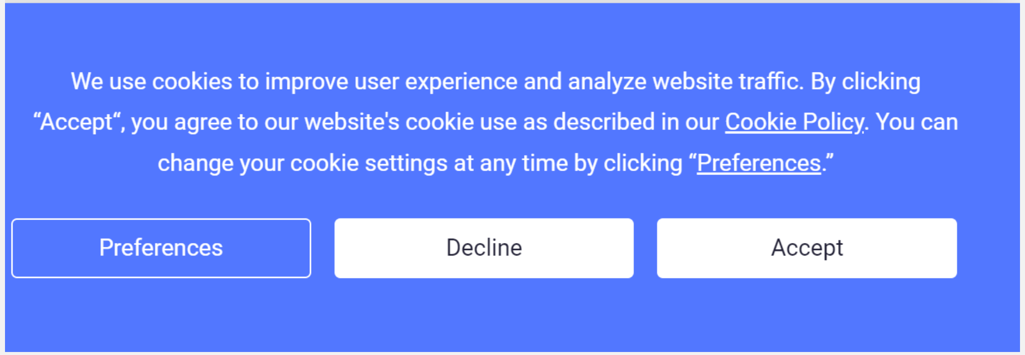
Revealed Value of Personal Data

US$/year, median value, n=180

SOURCE: Aricent/frog design, primary research (2011)

@ more-with-mobile.com

Cookies



We use cookies to improve user experience and analyze website traffic. By clicking "Accept", you agree to our website's cookie use as described in our Cookie Policy. You can change your cookie settings at any time by clicking "Preferences."

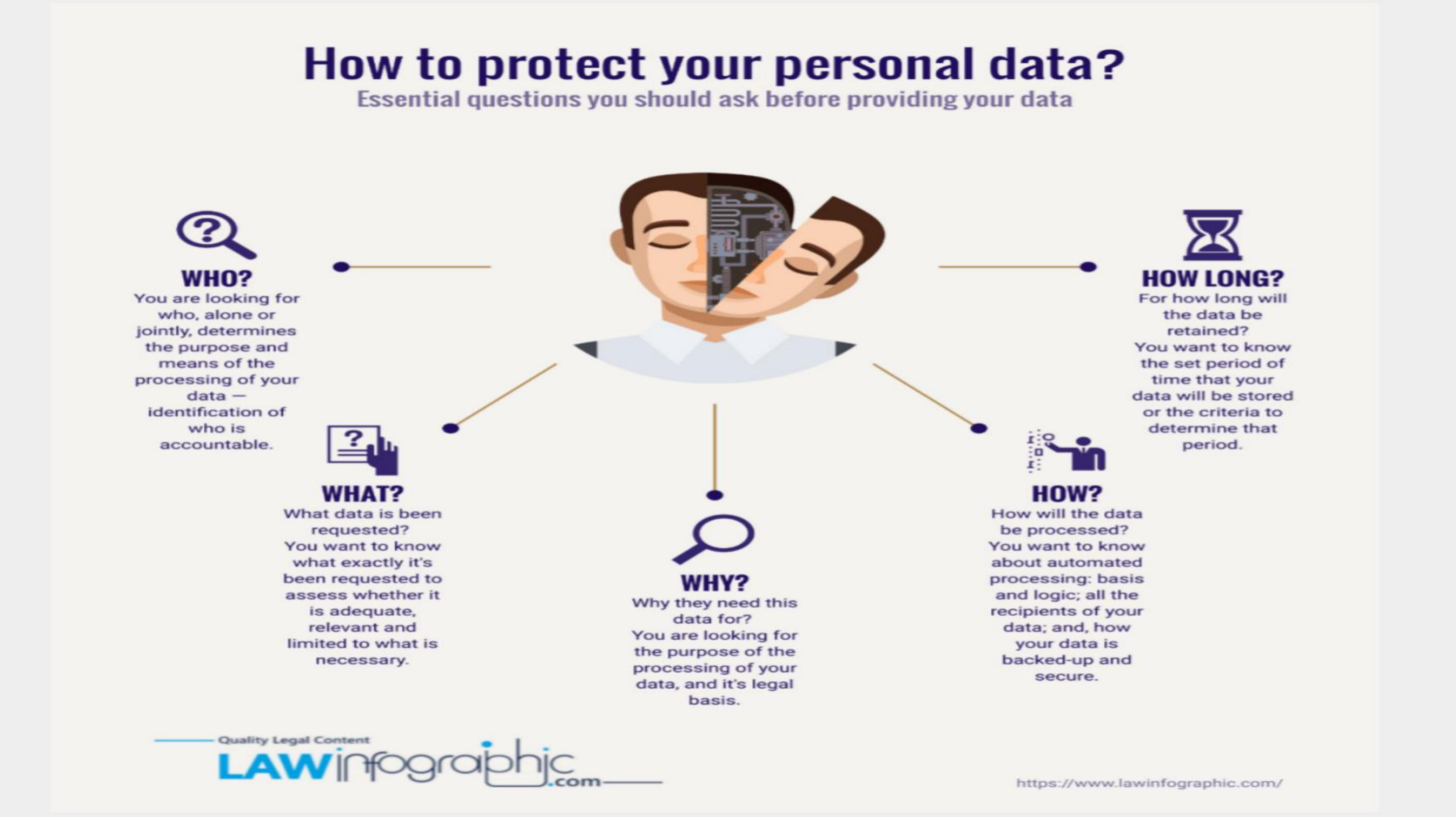
We do not accept all cookies. We protect our privacy.

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 behavior 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).

e-Learning Platforms and Privacy

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/	Kindergarten Primary/ 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/	Kindergarten Primary/ Secondary Education	E-mail account and password, two-factor authentication.	Yes
UK	Glow	https://glowconnect.org.uk/	Public Primary and Secondary	Being a teacher or education partner in Scotland	Yes

e-Learning Platforms and Privacy



How to protect your personal data?

Essential questions you should ask before providing your data

WHO?
You are looking for who, alone or jointly, determines the purpose and means of the processing of your data — identification of who is accountable.

HOW LONG?
For how long will the data be retained?
You want to know the set period of time that your data will be stored or the criteria to determine that period.

WHAT?
What data is been requested?
You want to know what exactly it's been requested to assess whether it is adequate, relevant and limited to what is necessary.

WHY?
Why they need this data for?
You are looking for the purpose of the processing of your data, and it's legal basis.

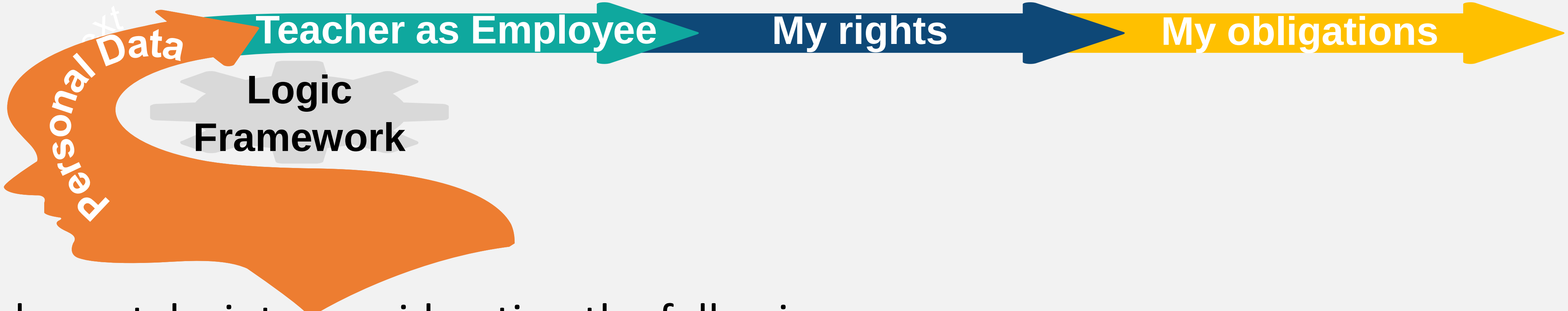
HOW?
How will the data be processed?
You want to know about automated processing: basis and logic; all the recipients of your data; and, how your data is backed-up and secure.

Quality Legal Content
LAWinfographic.com

https://www.lawinfographic.com/

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

The role of Teachers in the protection of personal data



We always take into consideration the following:

a) Identify which Personal Data of teachers and students are processed by the school.

b) Think of my Rights as a data subject.

c) Think of my obligations as an employee of the school for the process of students' personal data.

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

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.

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.

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.

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’.

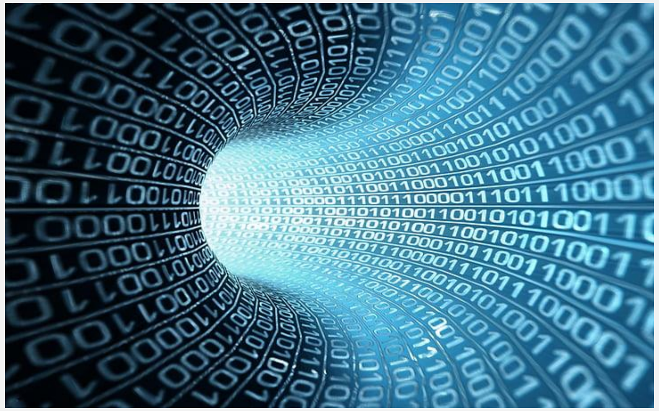
- When does the right to erasure apply?
  - The personal data is no longer necessary for the purpose that were collected;
  - Withdrawal of consent;

- In case of refusing to implement the request, we have the right to file a complaint to the component data protection authority.

The Right to Restrict Processing

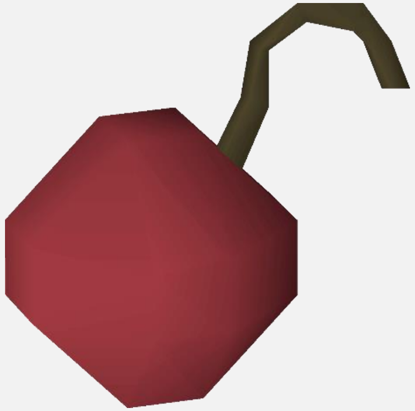
- We have the right to request the restriction of our data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, it is permited the storage of the personal data, but not the usage.
- The company/school shall answer within 30 days.
- We can ask the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

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.

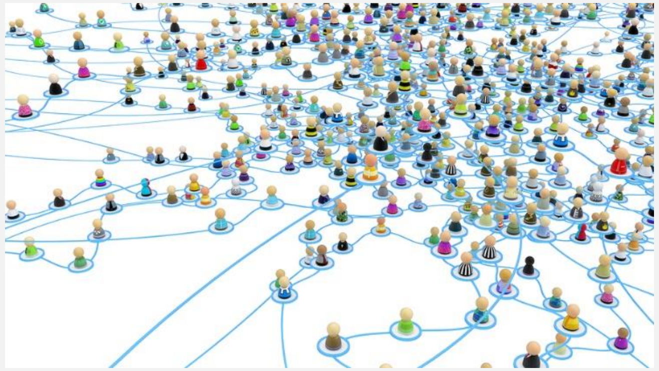
The Right to Object



- 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 immediatly using our personal data for advertising purposes (e.g., personalised ads in social media).

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

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.

Data Protection Officer

Αυτή η φωτογραφία από Άγνωστος συντάκτης με άδεια χρήσης CC BY-ND

We contact the Data Protection Officer in order to:

a. Get information about the processing of our personal data

b. Get information about the retention period

c. Submit a request for the fulfillment of our rights

d. Get information about the security measures taken

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 complain 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.

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 Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal	dpo@dataprotection.ro	+40 318 059 211 +40 318 059 212
UK	Information Commissioner’s Office	Scotland@ico.org.uk	+46 0303 123 1113

Teachers’ obligations related to Protection of Personal Data

Follow Data Controller’s instructions

Inform Data Protection Authority in case of a Data Breach

Obligation to inform Data Subjects

Be aware of Data Subjects Requests

We have the obligation to follow the written instructions of the school in the field of data protection

In case of a Data Breach we have to inform the School, the Data Protection Authority and the Data Subjects involved in the Breach.

We have the obligation to inform students about the process of their data and their rights, on behalf of the school.

When Students or their parents make requests related to Students’ personal data, we have to inform immediately the school.

Obligations of the Educational Institution (1/6)

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.

Obligations of the Educational Institution (2/6)

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.

Obligations of the Educational Institution (3/6)

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.

Obligations of the Educational Institution (4/6)

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.

Obligations of the Educational Institution (5/6)

Data Protection Officer

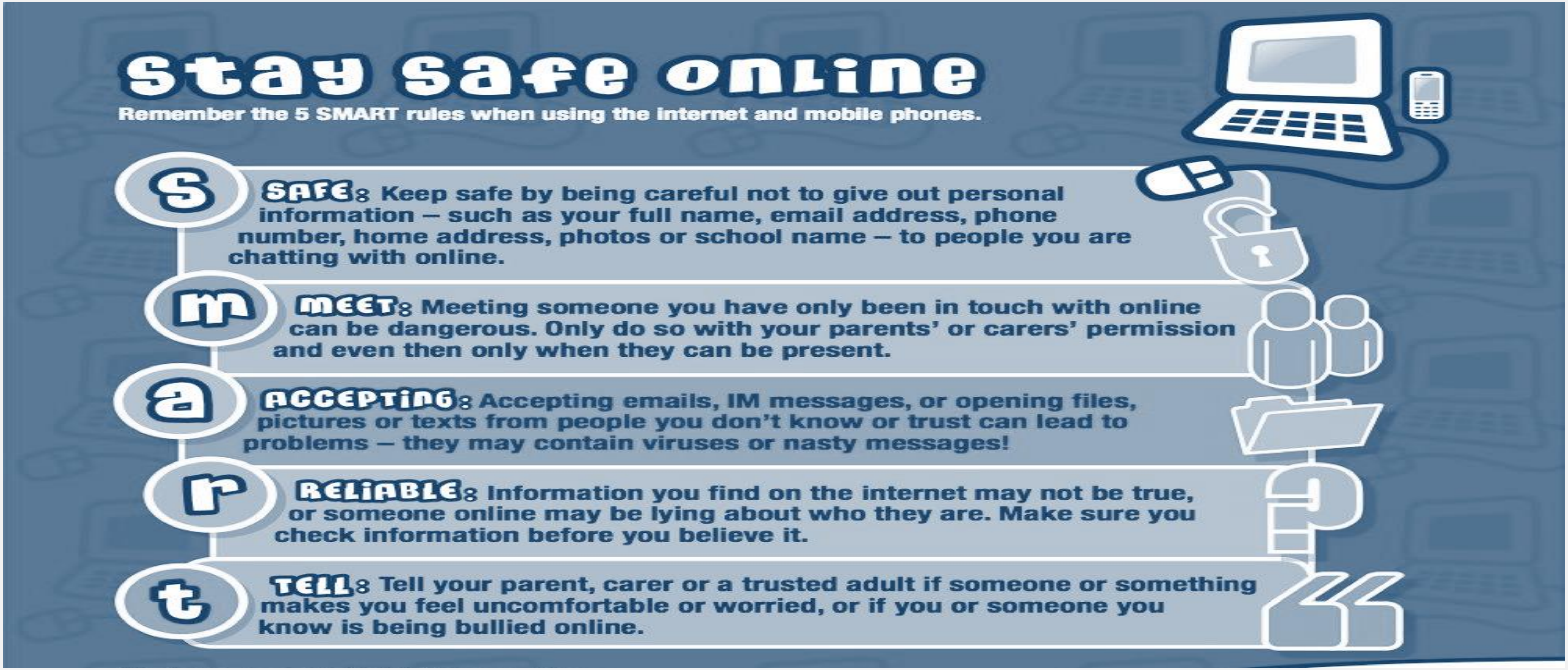
The educational organisation should appoint a Data Protection Officer to inform the data subjects about specific aspects of the process of personal data, to answer questions and concerns, and to raise awareness about data protection issues as well as to train teachers on the field of privacy and personal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

Obligations of the Educational Institution (6/6)

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.

Cybersecurity Tips



stay safe online

Remember the 5 SMART rules when using the internet and mobile phones.

S — **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.

M — **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.

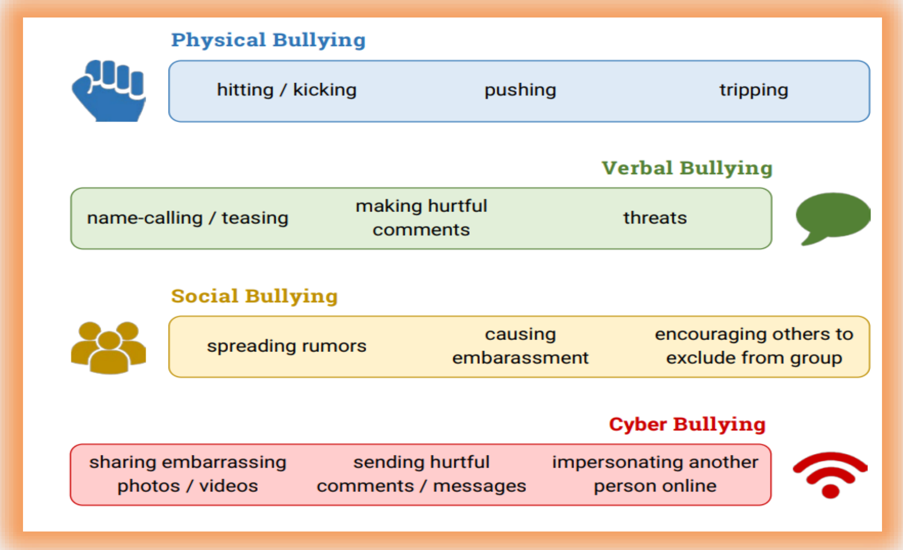
A — **ACCEPTING:** Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

R — **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.

T — **TELL:** Tell your 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.

What is Bullying and Cyberbullying?

- **Bullying** is purposeful, repeated behavior 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.



Physical Bullying

hitting / kicking | pushing | tripping

Verbal Bullying

name-calling / teasing | making hurtful comments | threats

Social Bullying

spreading rumors | causing embarassment | encouraging others to exclude from group

Cyber Bullying

sharing embarrassing photos / videos | sending hurtful comments / messages | impersonating another person online

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

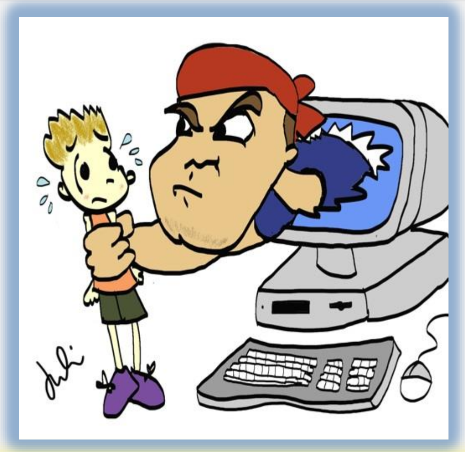
- intimidation and threats
- harassment
- exclusion or peer rejection
- impersonation
- unauthorized publication of personal information or images
- manipulation

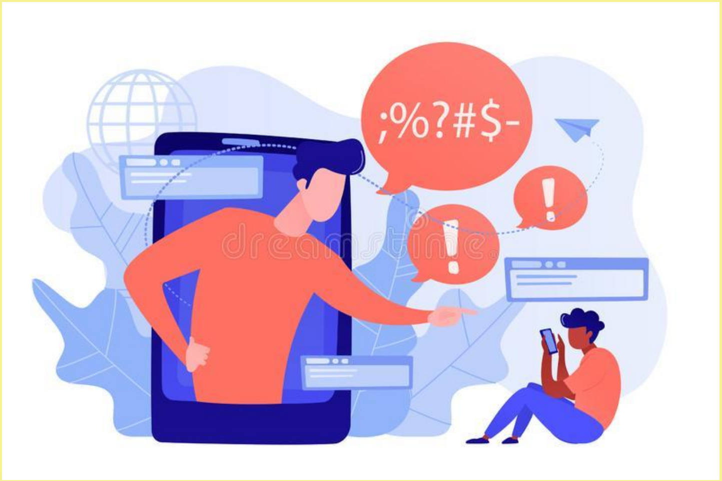
What kind of channels cyberbullies use?

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

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 down 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

be SMART ONLINE!

If you could be anything just be Kind

It will make you happy

It will help you build real friendships

Being mean is not cool

It is the right thing to do

Because anger creates more anger

Everyone is fighting their own demons

Kindness is a strength

Online Grooming (1/2)

Online Predators
"The planning required designing effective grooming strategies by an online child predator (aka, iPredator) correlates with their perverse objectives."
iΨ
www.ipredator.org

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

Online Grooming (2/2)

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.

Netiquette (1/2)

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.

Netiquette (1/2)

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!

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.

Types of Digital Footprints

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.

Digital Footprint

- 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.

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.

DIGITAL FOOTPRINTS

What do yours say?

BE CAREFUL ABOUT:

- What you share.
- Where you share.
- With whom you share.

BE SMART ABOUT:

- Sites you visit.
- Emails you open.
- Links you click.

BE YOURSELF

but be your best self.

Source: https://safesitter.org/digital-footprints/

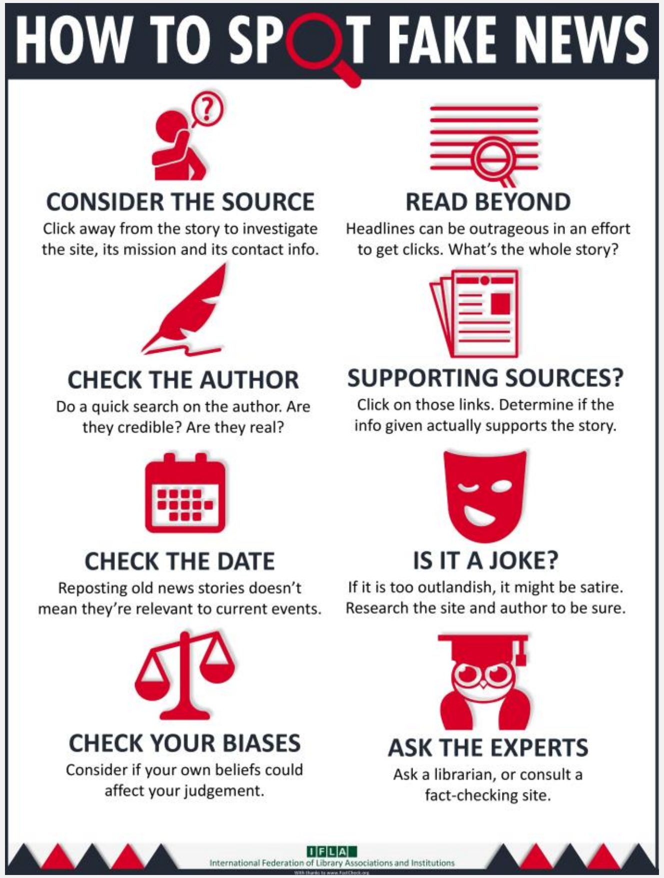
Digital Manipulation (1/2)

'image: Flaticon.com'. This cover has been designed using resources from Flaticon.com

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.

Digital Manipulation (2/2)



HOW TO SPOT FAKE NEWS

CONSIDER THE SOURCE
Click away from the story to investigate the site, its mission and its contact info.

READ BEYOND
Headlines can be outrageous in an effort to get clicks. What's the whole story?

CHECK THE AUTHOR
Do a quick search on the author. Are they credible? Are they real?

SUPPORTING SOURCES?
Click on those links. Determine if the info given actually supports the story.

CHECK THE DATE
Reposting old news stories doesn't mean they're relevant to current events.

IS IT A JOKE?
If it is too outlandish, it might be satire. Research the site and author to be sure.

CHECK YOUR BIASES
Consider if your own beliefs could affect your judgement.

ASK THE EXPERTS
Ask a librarian, or consult a fact-checking site.

IFLA
International Federation of Library Associations and Institutions
With thanks to www.FactCheck.org

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 behavior.

The Consortium

ΣΣ
ΣΤΑΜΑΔΙΑΝΟΣ
& ΣΥΝΕΤΑΙΡΟΙ
ΔΙΚΗΓΟΡΙΚΗ ΕΤΑΙΡΕΙΑ
HeartHands
SOLUTIONS
HANDS ON KNOWLEDGE
ATERMON
EDUCATIONAL PLAY
ΑΙΕΝ ΑΡΙΣΤΕΥΕΙΝ
ELLINOGERMANIKI
AGOGI
MAGNA CUM LAUDE - REUT FOUNDATION
founded in 1997
LAUDE-REUT
INTERDISCIPLINARY ACADEMY OF THE FUTURE

ePrivacing

2020-1-UK01-KA226-SCH-094506

IO2A1: e-Privacing Manual for Teachers

e-Learning and Personal Data

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

*This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*