

■ **Project:** 101132954—DRONE—ERASMUS-EDU-2023-PI-FORWARD

■ Teacher and school leaders training to promote Digital literacy and combat the spread of disinformation among vulnerable groups of

BEING SAFE IN AN UNCERTAIN WORLD

DEAR PARENTS!

As part of the DRONE project, we have created booklets for adolescents and parents to help combat disinformation:

- This booklet (**READING-4Parents**) is intended for parents, providing background information for conversations with children.
- Parents should discuss the **READING-4Adolescents** comic book with their children!
- **READING-4Teens** is intended for independent processing by older Adolescents.

In order to improve the materials, we welcome constructive feedback, which can be provided anonymously:



or <https://tinyurl.com/DRONEvj>

Thank you for your feedback!

This booklet for teenagers was created by the DRONE project in order to combat disinformation.

Created by the ELTE DRONE team using ChatGPT 5.0 on October of 2025 (v.2025.10.24):

- *Dr. Márta Turcsányi-Szabó, habil associate professor (tszmarta@inf.elte.hu), the Dean's commissioner for educational innovation at ELTE Faculty of Informatics*
- *Franciska Mikófalvy, ELTE IK T@T Kuckó coordinator*

Reading for parents

Parents play a key role in preventing the spread of fake news and misinformation within their families and communities.

Parents must learn to play role models and teach media literacy, encourage open and critical dialogue, supervise digital activities, promote responsible sharing, use educational resources, and collaborate with schools and other parents. In doing so, they empower their children to recognize, challenge, and resist fake news – thus increasing their resilience in the digital age.

To do this, parents need to learn and practice the following (see attachments):

Use and share educational resources

- **Being Up-to-date:**
Awareness of new forms of disinformation and the platforms where children spend time. Let's discuss which are reliable news sites, what each term related to disinformation means (see **A.** and **B. annex**).
- **Using games and tools:**
Use interactive resources, such as online tests, to help children recognize fake news in a safe environment (see **C. annex**).

Developing media literacy skills and practices (see **D.**, **E.**, and **F. annex**)

- **Understanding and teaching control:**
How to fact-check using reliable sources and encourage children to do the same. Practice together assessing the accuracy, manipulative nature and credibility of information, for example by using fact-checking websites and browser extensions.
- **Asking critical questions:**
How to ask about the source, perspective, and credibility of information.
How to think about: *Who made this? Why? Is it reliable? What might be missing or manipulated in it?*
- **Setting a good example:**
How to question sources, evaluate information, and recognize when you've made a mistake or shared false information. Avoid sharing unverified content!
- **Teaching responsible sharing:**
Make it a habit to verify information before sharing it and discuss the consequences of spreading false content.
- **Practicing social correction:**
What to do if a friend or family member shares fake news? How to approach the conversation in a kind and constructive way?

The importance of cybersecurity (see **G. annex**)

Cybersecurity means protecting your family's information, privacy, and devices while using the internet – especially now that artificial intelligence and online technologies have become commonplace.

- **Protecting personal information:** Children should be taught to protect their own and others' information (e.g. photos, names, school) and understand what are the risks of sharing it could lead to.

- **Preventing fraud and manipulation:** Online fraud and AI-based scams can target children. Children should be taught how to recognize suspicious messages and requests.
- **Prevent unauthorized access:** Strong passwords, privacy settings, and parental control tools can help prevent strangers from accessing your accounts.
- **Reducing the impact of AI data collection:** Artificial intelligence often collects data, in cases without our explicit consent. Children need to be educated to make informed decisions.
- **Developing smart digital habits:** Open conversations and good practices should help develop lifelong safe online behavior.

Monitoring and managing digital activities

- **Monitor and communicate exposure:**
Especially for younger children, set age-appropriate limits and use child-specific accounts when possible.
- **Guide, not blame:**
If your child comes across or shares questionable content, you should help and think through the content with your child, rather than correct or criticise your child for it. This is a good learning opportunity!

To promote open communication and critical thinking

- **Regularly discuss online content:**
Have ongoing conversations about what your child sees online - whether it's influencers, memes or viral stories. Use real-life examples, including your own experiences with fake news, to help make the topic more understandable.
- **Encourage openness:**
Be open to new ideas, listen to different opinions and admit when you're wrong.
- **Discuss peer pressure:**
Explain why people may share information they don't believe in because they want to fit in.

Collaboration with schools and the community

- **Support media literacy education:**
Support schools to teach media literacy and critical thinking as part of the curriculum.
- **Connect with other parents:**
Share your experiences and strategies with other parents to build a supportive community for responsible digital citizenship.

SUGGESTION: You can print out the pages of the annex individually and put them on the wall as posters to keep them in sight!

A. Annex: Auxiliary reading

"The truth is no louder than a lie — you just have to know how to hear it."

Parents should learn to model and teach media literacy, foster open and critical conversations, supervise digital activity, promote responsible sharing, use educational resources, and collaborate with schools and other parents. By doing so, they empower their children to recognize, question, and resist misinformation—building resilience against its spread in the digital age.

- **Media and Information Literacy Curriculum - E-version:**
<https://www.unesco.org/mil4teachers/en/curriculum>
- **Online Misinformation and Disinformation:**
<https://www.childrenandscreens.org/learn-explore/research/online-misinformation-and-disinformation/>
- **Family Guide to Misinformation and Disinformation:**
<https://digitalwellnesslab.org/family-guides/family-guide-to-disinformation-and-misinformation-online/>
- **How to Teach Teens to Navigate Misinformation:**
<https://parentandteen.com/how-to-teach-teens-to-navigate-misinformation/>
- **Protecting Children from Fake News:**
<https://www.internetmatters.org/issues/fake-news-and-misinformation-advice-hub/protecting-children-from-fake-news/>
- **Online Safety Guide for Parents:**
<https://www.wirral safeguarding.co.uk/online-safety-guidance-parents/>
- **How to talk to your family about fake news:**
<https://www.bbc.co.uk/bitesize/articles/znf4bqt>
- **How to tackle misinformation when it's coming from a loved one:**
<https://www.edf.org/how-tackle-misinformation-when-its-coming-loved-one>
- **Microsoft Family Safety Toolkit:**
<https://msblogs.thesourcemediassets.com/sites/5/2024/02/2024-Microsoft-Family-Safety-Toolkit.pdf>
- **AI Companions Pose Risk to Teens:**
<https://www.aiforeducation.io/blog/ai-companions-pose-risk-to-teens>
- **Understanding Cybersecurity - Beginners' Course:**
<https://www.teensinai.com/understanding-cyber-security/>
- **Google - Empowering your family to safely play online:** <https://families.google/>

B. Annex: Baseline concepts

Digital Literacy: The ability to use digital tools and technologies effectively, safely and critically.

This includes skills such as evaluating online information, browsing websites, using applications, and understanding digital rights and responsibilities.

Cybercrime: A crime committed using computers, smart devices, or the internet. These can include online attacks, fraud, data theft, or harassment – any activity that takes place in the digital space and violates the law.

Cybersecurity: The protection of digital systems, networks, and data from unauthorized access, attack, or damage.

Includes using secure passwords, recognizing online threats, and monitoring safe online behavior.

Critical Thinking: The ability to think clearly and logically, question assumptions, evaluate evidence, and draw sound conclusions.

Essential for making informed decisions and defending against misinformation.

Disinformation: Intentionally false information created and disseminated to deceive or mislead people.

Example: Fake news intended to manipulate public opinion.

Misinformation: False or inaccurate information that is not intentionally shared with the intent to mislead.

Example: Sharing a poorly captioned image in the belief that it is true.

Malinformation: Real information that is used to cause harm to a person, organization, or country.

Example: Leaking confidential information to embarrass someone.

Fake news: Made-up news presented as legitimate journalism, often spread on social media.

Example: Viral headlines claiming false scientific discoveries.

„Deepfake”: Synthetic media (usually video or audio) generated by AI to imitate real people, often in a convincing way.

Example: A video of a politician saying things he never said.

Algorithmic amplification: The way social media platforms' algorithms increase the visibility of certain content — sometimes unintentionally helping to spread misinformation.

Example: Sensational or misleading posts going viral due to algorithms that focus on engagement.

Echo chamber: An online environment where people only encounter opinions that reinforce their own, limiting critical thinking.

Example: A social media feed that presents only one political viewpoint.

Confirmation bias: The tendency to believe or share information that confirms our existing views, regardless of its truthfulness.

Example: Ignoring credible sources that contradict a favored opinion.

Media Literacy: The ability to critically analyze and evaluate media content, source intentions.

It is crucial for students and adults to recognize and challenge disinformation.

Fact-checking: Verifying information with trusted sources before sharing or publishing it. Organizations like Snopes and PolitiFact can help with this.

Source Reliability: Judging the reliability of a source based on its history, expertise, and transparency.

Example: Using information primarily from peer-reviewed journals rather than anonymous blogs.

Digital footprint: All the data a person leaves behind on the internet, including shared content, comments, and posts.

Sharing consciously helps limit the spread of harmful content.

Cybersecurity Awareness: Understanding digital threats, including disinformation, as part of protecting individuals and institutions online.

Includes recognizing phishing, manipulation, and media forgery.

Hate Speech: Speech, writing, or content that attacks a person or group on the basis of race, religion, ethnicity, politics, gender, sexual orientation, or other identity with hatred or incitement to violence.

Example: "All [ethnic groups] are only bringing us trouble, they should be banned from the country!"

Bias: A conscious or unconscious bias that favors one gender over another, for example — often negatively affecting women or non-binary people in the media, workplace, decision-making, etc.

Example: An article describes a male leader as "assertive" and a female leader as "dominant" for the same behavior.

Trolling: Intentionally provocative, hurtful, or misleading online comments intended to provoke an emotional response or stir up controversy.

Example: Someone writes under a conservation post: "I hope they cut down all the trees, what are they for?"

Clickbait content: A misleading or overdramatized headline that entices the reader to click on it—even if the content doesn't deliver what the headline promises.

Example: "Your favorite actor did something shocking—you won't believe your eyes!" (The article reveals that he was just giving an interview.)

How to Spot Disinformation:

C — Check the Source

*Is it a credible news site or just a random account?
Does the website end in “.com.co” or “.xyz”? (That’s often a red flag.)
Do other, more trustworthy outlets report the same story?
Tip: On social media, always check who posted it first!*

H — Has It Been Properly Referenced?

*Does it cite a real, verifiable source?
Sometimes posts mention “scientific data” that either doesn’t exist or actually proves something else.
Tip: Always find and read the original source before believing or sharing.*

E — Expired or Outdated?

*Maybe the event really happened—but years ago.
Old stories are often reshared as if they’re breaking news.
Tip: Always check the date or timestamp!*

C — Check with Verification Tools

*Use fact-checking and image search tools to verify suspicious content.
These tools can show where a photo or video originally came from.
Tip: Collect some basic online verification tools—you’ll need them!*

K — Keep Calm and Read Beyond the Headline

*The headline might be clickbait.
Is the story really about what the headline claims?
Is it full of ALL CAPS, exclamation marks, or overly emotional language?
Tip: If it sounds too shocking to be true—it probably isn’t.*

E — Examine the Visuals

*Zoom in on photos and videos.
Look for odd details—hands, eyes, or shadows that don’t look natural (AI often messes these up).
Does the mouth match the voice? Are jewelry and details consistent?
Tip: Watch videos with sound off—if it still looks “off,” it might be fake.*

R — Realistic and Reasonable?

*Does it actually make sense?
Is there exaggeration, sensationalism, or “too good/bad to be true” language?
Tip: Truth spreads slowly—fake news spreads fast.*

Be a **C.H.E.C.K.E.R. — verify before you share!**

D. Annex: Disinformation games

"It's better to play it than to live it and be scared!"

1. Bad News Game

 <https://www.getbadnews.com/>

An interactive, English-language game where we can become fake news producers ourselves to learn what tricks are used to manipulate the internet.

Goal: to recognize manipulation techniques (clickbait, deepfake, emotional language, etc.).

- ✓ Interesting for young people and parents alike.
- ✓ Simple English

2. BBC iReporter

 <https://www.bbc.com/news/school-report-43391188>

BBC's playful simulation where you can be the news editor and decide what to share on social media.

Challenge: recognize fake news and false content.

- ✓ Interactive, story-based learning
- ✓ Develops media awareness

3. Spot the Troll Quiz

 <https://www.spottthetroll.org/>

An online quiz where we have to decide whether a social media profile belongs to a real person or a troll account.

Objective: to develop critical thinking, to learn to notice artificially stirred up discussions.

- ✓ Interesting for adults too
- ✓ Good conversation starter within the family

4. InVID & WeVerify Toolkit

 <https://www.invid-project.eu/tools-and-services/invid-verification-plugin/>

An extension that allows you to check the origin of images and videos, for example, suspected deepfake content.

How to use: a bit more technical, but with parental help, even children can understand.

- ✓ A more serious but useful tool
- ✓ Can also be used in education

5. Real or Fake: Can You Spot Misinformation?

 <https://judgegpt.streamlit.app/>

Real or Fake: Can you spot false information?

- ✓ Good for parents and older adolescents

E. Annex: Examine yourself for parents

"I'm sure I know: what do I know?"

Task: Please rate how confident you feel in the following areas on a scale from 1 to 5:

- 1 = Not confident at all
- 2 = Slightly confident
- 3 = Moderately confident
- 4 = Confident
- 5 = Very confident

No. – Statement | Check the appropriate box! 1 | 2 | 3 | 4 | 5

I can help my child create strong and secure passwords.

☐☐☐☐☐

I understand how to turn on and explain two-factor authentication (2FA).

☐☐☐☐☐

I can recognize and explain what phishing scams look like.

☐☐☐☐☐

I know what a digital footprint is and why it matters.

☐☐☐☐☐

I am prepared to talk with my child about fake news and misinformation.

☐☐☐☐☐

I can recognize AI-generated content (e.g., deepfakes or fake images).

☐☐☐☐☐

At home, I set an example by sharing responsibly and fact-checking information.

☐☐☐☐☐

I know how to properly guide my child (without judgment) if they make a mistake online.

☐☐☐☐☐

I use tools or websites to verify whether online information is true.

☐☐☐☐☐

I cooperate with my child's school or other parents on digital safety or media literacy topics.

☐☐☐☐☐

Reflection

Summarize your scores.

Any item marked with a 1 or 2 can be a good starting point for further learning.

Scores of 4 or 5 indicate confidence — well done!

If not, please read all the attachments carefully!

☒ **Would you like to improve further? Review the materials included in the file!**

F.Annex: Fact checking tools

Reliable online tools to check for fake content

1. Google Fact Check Explorer

<https://toolbox.google.com/factcheck/explorer/search/list:recent:hl=hu>

A search engine that shows you if a statement has been verified.
Great for checking quotes or news.

✓ Official Google tool, also used by journalists.

2. InVID WeVerify Toolkit

<https://www.invid-project.eu/tools-and-services/invid-verification-plugin/>

Browser extension that verifies the origin of videos and images.
Performs reverse image search, checks for deepfake signals.

✓ Trusted by European media professionals.

3. TinEye

<https://www.tineye.com/>

Reverse image search: by uploading an image, it will show you where it came from.
Helps identify old images that are used for fake news.

4. Snopes

<https://www.snopes.com/>

It exposes false rumors, fake news, and scams.
Simple, easy-to-understand explanations - perfect for teens too.

✓ A trusted source for over 20 years.

5. Media Bias/Fact Check

<https://mediabiasfactcheck.com/>

It shows how biased or trustworthy a news site is.
It rates the sites on a scale and provides an explanation.

G. Annex: Genuine Dialogue

"We are one team."



Give the children the story to read, then start a conversation:

- Have you ever encountered a similar situation?
- How did you handle it?
- Mention situations where more background knowledge was needed to handle the case properly.

Characters:

Lia (14): Friendly, open, loves to dance, regularly posts on TikTok.

Rafi (15): Lia's cousin, quiet and tech-savvy.

Miss Smith: A cool librarian who runs the school's digital club.

Chapter 1: The viral tag

Lia was excited. Her latest dance video had just reached 10,000 followers on TikTok. Over 18,000 views in two days. Then a **tag** came.

"Omg, you slayed this 🤩 check this out too!" - and a strange link.

She clicked on it. Nothing loaded. "Hmm, maybe it's broken." She didn't think anything more about it.

Chapter 2: Something... is not right

Later that night, one of her friends texted her:

"Hey... did you send me a weird video??"

Then another message:

"Why are you texting everyone about winnings? Your account was hacked?"

Lia's stomach churned. Her TikTok was messaging her followers, and she didn't know about it.

Lia panicked and called her cousin Rafi.

"Don't worry," Rafi said. "This happened to another friend of mine too. It's called phishing."

"Phishing?!" Lia blinked.

"Not with a fishing rod. It's when scammers 'fish' for your info. That link probably tricked your app into letting them in."

They set a new password, turned on two-factor authentication (2FA), and Rafi helped them report the issue.

"But why me?" Lia asked.

"Because you clicked on it," Rafi said gently. "It happens to smart people too."

Chapter 3: The Digital Club

The next day, Lia went to the school library still upset. Miss Smith, the librarian, noticed her. Lia told her everything.

"I didn't even think about it. There was only one member. I feel so stupid."

Miss Smith smiled kindly.

"You're not dumb. You're learning. That's why we started the Digital Life Club. Will you join?"

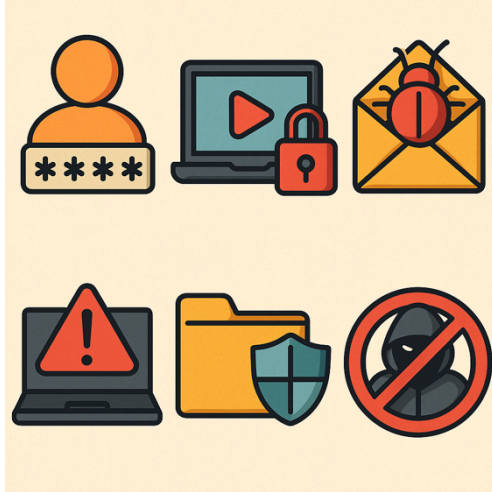
Chapter 4: What I learned

A week later, Lia stood in front of the Digital Club.

"It's scary how quickly it happened. But I realized... I've never really thought about how I use social media." She held up her list...

Why Cybersecurity Matters (Yes, to You Too!)

"Cybersecurity is not about fear, it's about freedom: being able to be yourself, share, connect, and create without being bothered."



What is cybersecurity anyway?

Think of cybersecurity like personal hygiene - just for your digital life.

Just as brushing your teeth protects you from cavities, cybersecurity protects you from:

- Hackers stealing your account
- Strange strangers seeing your data
- Losing your photos, homework, or even your identity

And no - you don't have to be a famous influencer to be targeted. If you're online, you're already in the "game."

What can happen if you don't protect yourself?

- Your TikTok or Insta account is hacked and spammed,
- Your email is used to reset other passwords,
- Personal photos or messages are leaked,
- Someone impersonates you and scams others,
- Your private messages become public,
- Your school emails are hacked
- Someone places orders in your name
- You are blamed for messages you didn't send.

😬 Yes, this really happens. It's not just an "adult problem."

How can you defend yourself?

- Protect your accounts!
- Use a strong password and don't use the same password everywhere!
- Don't fall for psychological manipulation!
- Be aware of AI's disinformation reinforcement methods!
- Always use Netiquette!
- Minimize your digital footprint!
- Be a constant CONTROLLER!
- Don't be afraid to report when others don't follow protective rules!
- Learn about the types of negative information!
- Learn what's cool and what's ugly about AI!
- Understand why overuse of AI can be dangerous for students!
- Understand why learning is important (even alongside AI)!

----- More about these will be discussed later!

How to stay safe on social media?

“Social media is YOUR space. You control it!”



Social media can be great for having fun, chatting with friends, and sharing memes – but it can also easily become chaotic. Hackers, bullies, weird private messages, and fake content are everywhere. Here's how to stay safe and strong online:

1. Think ahead!

Everything you post can be saved - even if it disappears afterwards.

🧠 Don't share too much personal info, like school, home, location, or daily routines!

2. Block and mute = it's self-defense

If someone sends you weird, hateful, or just annoying things — block them immediately!

3. Lock your accounts

-Private account = your power: Set it so that only you decide who can follow you. Use face recognition, fingerprint or PIN code on Windows: Settings → Accounts → Sign-in options: ask for PIN, fingerprint, face recognition after password.

-Two-factor authentication (2FA): Always turn it on. If someone gets your password, they still won't be able to log in without the second code.

➡ Activating 2FA:

Windows: <https://account.microsoft.com/security> „More security settings” → “Set up two-step verification”

(must be installed on mobile and confirmed with Microsoft account via notification or code).

Android: “Settings” → “Google” → “Security” → “Two-step verification”

→ You can choose SMS, email or Authenticator

-Use a password manager! (e.g. Bitwarden, 1Password)

4. Beware of phishing or fake links

Do you get a message saying, “OMG, is this you??” and a link? 🚨 DON'T CLICK!

This is usually a trap to steal your account.

🧠 Only click on links that you feel are trustworthy. If they look suspicious, they probably are.

5. What to do if attacked

Don't respond. That's what they want.

Take a screenshot of everything. Evidence counts. Block and report.

➡ How to take a screenshot:

Windows: PrtScn (PrintScreen)

Android: Power Button + Volume Down (may vary by manufacturer)

→ Photos → Screenshots

➡ How to report:

On Instagram, TikTok, X, Snapchat, etc.:

Tap the three dots (...) next to their profile or post

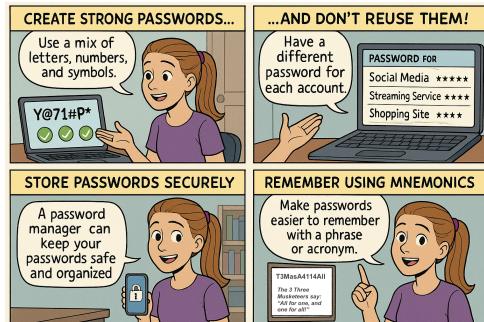
Select "Report" or "Report User"

Follow the instructions!

🧠 If it's serious (threats, harassment, blackmail), tell an adult and report it to your local cybercrime authorities.

Smart password usage for teens

“Treat your passwords like your secrets: keep them strong, unique, and *DO NOT* share them.”



1. MAKE: Strong and smart passwords Use this formula:

- At least 12 characters
- Mix uppercase and lowercase letters, numbers, and symbols
- Convert words: i = 1, v = 5,
- Do not use personal information (such as your name, date of birth, pet name)

TIP: Make a sentence into a password:

“My dog barks at 7 PM!” → Mdba7PM!

2. MAKE A DIFFERENCE: One password ≠ all accounts

Never use the same password for multiple apps or websites.

If one is compromised, they are all at risk. Use small modifications if you have to:

Instagram → Foto\$Insta2025!

School email → Learn&grow2025!

🧠 Be smarter: use different passwords. That way, if one lock is compromised, the others will remain safe.

3. STORE: Where to keep it safe

DO:

Use a password manager (e.g. Bitwarden, 1Password, or your browser's secure vault).

Only write it down if it's in a locked account or private notebook.

DON'T:

Don't save it in a note or Word document on your phone or computer.

Don't share it in a message, chat, or screenshot.

4. REMEMBER: Train your brain

Use patterns, rhymes, or visual tricks to remember important passwords.

Example: For school: “Books<3@” → Image: 📚 + ❤️ + 🧠

Test yourself every few weeks.

TREAT: Keep it a secret

Your password is like your toothbrush:

Only you use it!

Change it if it's old, shared, or leaked

Don't share it with your friends, even your best friends.

If you have to share it (e.g. family Netflix), create a separate account or profile.

Bonus Tip: Watch out for this...

Password requests in emails or messages = phishing

Strange-looking login pages = fake websites

Random pop-ups = malware traps

Check the URL (web address) and enable two-factor authentication (2FA) when possible.

Check sometimes - have they been hacked:

🔗 <https://haveibeenpwned.com/>

By entering your email address, we can find out if it has been hacked.

What is social engineering and why is it important?

"If someone urges you, guilt-trips you, or intimidates you...it's a trap."



Social engineering occurs when someone tries to trick you into giving them your personal information, passwords, or even access to your accounts. It's like digital manipulation. It's not your device that's being "hacked," it's you that's being "hacked."

Common social engineering tricks:

Phishing: Fake messages or emails:

"OMG, is this you in this video?"

"Click here to get your free prize!"

"Your account has been suspended, log in now!"

Impersonating someone:

A "friend" asking for your password.

Someone saying, "I'm the school administrator, can I reset your password?"

Emotional pressure:

"If you don't respond in 5 minutes, there's going to be trouble."

"You'll be banned if you don't click now!"

Here's how to protect yourself professionally:

1. Slow down! Always.

If the message is urgent, emotional, or strange — stop and think.

Scammers want you to act quickly without thinking.

Slow = safe. Fast = risky.

2. Never share personal information

Passwords, codes, addresses, or school information don't go over MS or SMS - even with "friends."

If someone really needs help, they will call or talk to you in person.

3. Double-check the source

If a friend sends you a strange link, ask, "Did you really send this?"

Check email addresses — for example, support@instagram.com is not the same as insta-help4421@gmail.com

4. Use two-factor authentication (2FA)

Even if someone gets your password, they won't be able to log in without the second code, which will be sent to your phone or email.

✓ Don't be shy to report

Have you been scammed? It happens to smart people too.

Report fake messages on social media (tap ... > Report)

Tell a trusted adult, teacher, or school administrator.

How AI could accelerate cybersecurity threats (and what you can do about it)

“AI can copy voices, make fake videos, and write realistic scams, but it can’t replace your critical thinking. That’s your real strength!”



What is AI?

AI (Artificial Intelligence) is like a super smart computer brain. It powers things like:

- Chatbots
- Facial recognition
- Smart assistants (like Siri or Alexa)
- Even TikTok’s “For You” page

AI can be used for good or bad purposes.

How bad guys use AI to break in or scam you

Smarter scams:

AI can write super realistic messages that sound like they were written by your friends, your school, or even your parents.

Example: “Hi, it’s Mrs. Szabó from school — click here to recover your account.”

Warning: fake.

Fake images and videos (deepfakes)

AI can create fake faces, voices (even mimicking the voices of real people!) or videos that look real — to deceive or embarrass people.

Mass attacks

AI can automatically send thousands of phishing emails or messages, hoping someone will fall for them.

Chatbots that pretend to be humans

You may be talking to a bot, not a human - and it may have been trained to trick you into giving it information.

Think before you believe everything

If you see a crazy video or shocking message, check the facts.
Ask yourself, “Could AI have made this?”

Extra tip: AI can help you too!

AI isn’t just a threat — it’s also used for defense:

- Spam filters in emails
- Facial recognition on your phone
- Recognizing suspicious logins on Instagram or TikTok

Netiquette for adolescents

“The online space is like a digital neighborhood”

NETIQUETTE FOR ADOLESCENTS

PROTECT YOUR PRIVACY



Pause before posting or sharing, using strong passwords and 2FA

If you wouldn't shout it in a crowded room, don't post it online.

THINK BEFORE YOU TYPE



Pause before posting, commenting or sharing.

- Would I say this to someone's face?
- How would I feel if this were about me?

The delete button exist, but screenshots are forever.

BE KIND. BE RESPECTFUL. BE HUMAN.



Avoid oversharing feelings or venting in public threads.

- Talk to a trusted friend or adult offline when upset.
- Don't vague posting to "get back" at someone.

digital drama is exhausting-and public.

USE YOUR PLATFORM FOR GOOD



Share things that inspire, uplift or educate.

- celebrate others' success
- Spamming, chain messages, excessive tagging, public shaming or calling out is not cool

Mental health > nonstop scrolling

NO DRAMA. NO DUMPING.



Not everything online is true

- Avoid spreading rumors, fake news or scary trending hoaxes
- Report hate. Your voice matters- use it wisely.

AVOID THESE ONLINE BEHAVIORS



- Tell a trusted adult
- If you feel unsafe
- public shaming or calling out

SET BOUNDARIES AND TAKE BREAKS



- Don't compare your real life to other peoples highlight reels
- use screen time settings or take social media breaks if needed

WHEN THINGS GO WRONG-SPEAK UP

tell a trusted adult- it's never "just drama" if it hurts.

You're not alone!

1. Protect your privacy

Don't share personal information like your full name, school, address, phone number, or daily routine. Use strong, unique passwords and enable two-factor authentication (2FA).

Keep your accounts private, and be specific about who can see your posts.

2. Think before you type

Stop before you post, comment, or share something. Ask yourself:

“Would I say this to someone face to face?”

“How would I feel if it was about me?”

Avoid sarcasm or dark jokes — they may not always be understood the way you think.

The delete button exists, but screenshots remain.

3. Be kind. Be respectful. Be human.

Treat others the way you want to be treated — even online.

Don't be a troll. Don't feed the trolls.

Stand up for others and report bullying to an adult.

4. Use your platform for good

Share inspiring, uplifting, or educational content.
Celebrate the successes of others. Support your friends.
If you see hate, report it.
Your voice matters - use it wisely.

7. Set boundaries and take breaks

Feel free to switch off and relax.
Don't compare yourself to other people's glamorous lives.
Use screen time settings or take a break from social media.

5. No drama. No dumping.

Avoid over-sharing emotions or complaining in public forums.
If you are upset, talk to a trusted friend or adult in person.
Don't post vaguely.

8. When things go wrong-Speak up

Tell a trusted adult if:
You don't feel safe, someone is threatening or harassing you, or you've seen or experienced harassment. Report abuse using the app's built-in tools (Instagram, TikTok, Snapchat all offer a "Report" option)!

Check the sources

Not everything on the internet is true.
Avoid spreading rumors, fake news, or scary "trendy" fake stories.
If it sounds too shocking, funny, or dramatic - it probably is.

Ask permission before posting other people's pictures

Accept if they say no.

Don't share embarrassing photos or videos – even if you mean it “just for fun.”

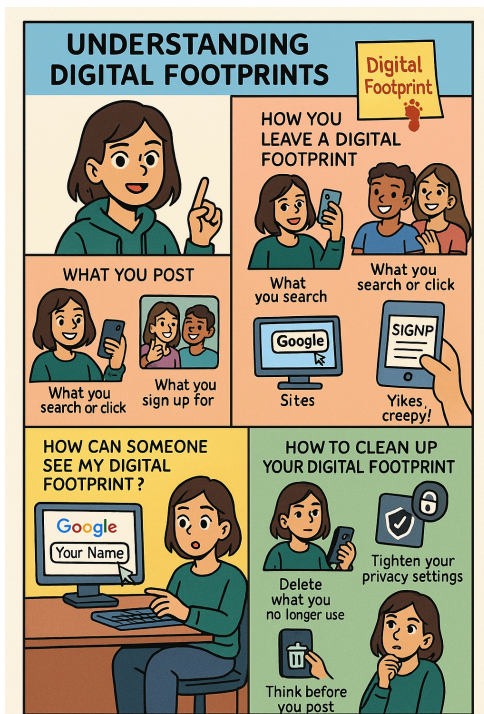
6. Avoid these online behaviours

Cyberbullying (harassment, exclusion, identity theft)
Ghosting (when someone suddenly, without any explanation, breaks off contact with another person, becoming a ghost) without justification
Spam (unsolicited or mass messages, usually sent by email and are malicious)
Public shaming or “name calling”.

Understanding digital footprint (and why it should be addressed)

ELTE
EÖTVÖS LORÁND
UNIVERSITY

“Your digital footprint is like a tattoo on the internet — make sure you’re proud of it.”



Every time you go online — whether it’s posting a selfie, liking a video, searching for something on Google, or connecting to Wi-Fi — you leave behind tiny traces.

We call these traces your digital footprint. It’s like walking in the snow: every step you take leaves a mark. It only happens here on the internet, and it can last forever.

How do you leave a digital footprint (without realizing it)?

What you post: Photos, videos, captions and comments, stories, introductions, usernames, hashtags.

What others post about you: Group photos you’re tagged in, posts that mention your name or school.

What you search for or click on: Google searches, links you click, videos.

What you sign up for: Social media accounts, online games, quizzes, sweepstakes, apps.

How someone can see your digital footprint?

Type your name into Google — what comes up?

Your friends, schools, and even future workplaces will do the same.

Ads and companies track your clicks and likes to build a profile of you (what you like, what you buy, what you watch).

The Internet DOESN'T Forget - See what it has saved about you:

- <https://web.archive.org/> - **Time machine:** what did it save?
- <https://archive.ph/> - preserves dynamic pages as well
- <https://timetravel.mementoweb.org/> - archive aggregator: search in multiple places

How to clean (and manage) your digital footprint:

1. Google yourself regularly

Search your name in quotation marks: “Your name” + city or school.

If you find something strange, request that it be removed.

2. Tighten your privacy settings

Make your accounts private. Only friends should see your posts. Turn off location tagging. Try this: Instagram, TikTok, Google & YouTube → Settings → Privacy

3. Delete what you no longer use

Old accounts? Close them. Unused apps? Delete them. Weird posts? Remove them.

4. Think before you post

Ask yourself: “Would it be okay if my teacher, my grandma, or my future boss saw this?”

5. Use cleaner tools

Use a privacy-focused browser (for example DuckDuckGo: <https://duckduckgo.com/>)

Regularly delete your search and location history

Use a password manager to reduce risky logins!

How to spot fake news, deepfakes and disinformation **CHECKER**

"Don't believe what you see — think before you share."



What is disinformation?

Disinformation = intentionally spread false information intended to confuse, deceive, or divide people.

C — Check the Source

Is it a credible news site or just a random account? Does the website end in ".com.co" or ".xyz"? (That's often a red flag.) Do other, more trustworthy outlets report the same story?

Tip: On social media, always check who posted it!

H — Has It Been Properly Referenced?

Does it cite a real, verifiable source? Sometimes posts mention "scientific data" that either doesn't exist or actually proves something else.

Tip: Always find and read the original source before believing or sharing.

E — Expired or Outdated?

Maybe the event really happened—but years ago. Old stories are often reshared as if they're breaking news.

Tip: Always check the date or timestamp!

C — Check with Verification Tools

Use fact-checking and image search tools to verify suspicious content. These tools can show where a photo or video originally came from.

Tip: Collect some basic online verification tools—you'll need them!

K — Keep Calm and Read Beyond the Headline

The headline might be clickbait.

Is the story really about what the headline claims?

Is it full of ALL CAPS, exclamation marks, or overly emotional language?

Tip: If it sounds too shocking to be true—it probably isn't.

E — Examine the Visuals

Zoom in on photos and videos.

Look for odd details—hands, eyes, or shadows that don't look natural (AI often messes these up).

Does the mouth match the voice? Are jewelry and details consistent?

Tip: Watch videos with sound off—if it still looks "off," it might be fake.

R — Realistic and Reasonable?

Does it actually make sense?

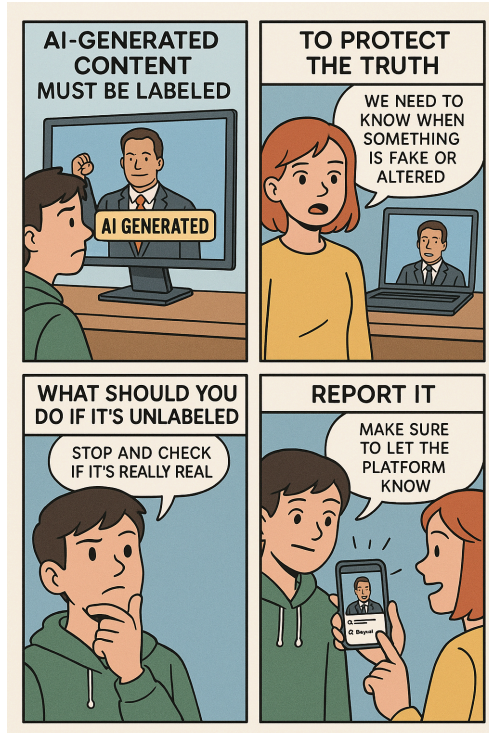
Is there exaggeration, sensationalism, or "too good/bad to be true" language?

Tip: Truth spreads slowly—fake news spreads fast.

Be a C.H.E.C.K.E.R. — verify before you share!

Why should AI-generated content be labeled — and what to do if it's missing?

"If you know what's real, it's easier to think for yourself."



What is AI-generated content?

AI-generated content refers to photos, videos, audio recordings, or text that are created or edited by artificial intelligence, rather than real-life events.

Some examples:

- A video of a celebrity saying something they never said
- A photo of a protest that never actually happened
- A "voice message" that sounds like it's from your teacher but was actually made by a bot

Why it needs to be labeled

The European Union requires that AI-generated content be clearly labeled for the following important reasons:

1. To protect the truth

Without labels, people can't tell what's real and what's fake. Deepfakes can be used to lie, deceive, or hurt. Labeling helps you decide what to believe.

2. To prevent manipulation

AI can spread fake stories during elections, wars or emergencies. Tags stop panic, fear or unfair influence. Your opinion matters - don't let a fake video shape it.

3. To build trust

Artists, influencers, and brands who use AI are honest. This shows that they don't want to deceive anyone. Honesty online = a safer internet for everyone.



What to do if you find unlabeled AI content?

Stop and think before sharing!

If it seems too shocking, dramatic or strange - don't share it yet.

Double-check it!

Report: On TikTok, YouTube, Instagram or X (Twitter):

Tap the three dots (...) on the post

Select the "Report" option

Select something like "Misleading or manipulated media"

You are not betraying - you are defending the truth.

How AI can help spread negative information

"Not all that glitters is gold!"



Algorithmic amplification: The way social media platforms' algorithms increase the visibility of certain content — sometimes unintentionally helping to spread misinformation.

Example: Sensational or misleading posts going viral due to algorithms that focus on engagement.

Echo chamber: An online environment where people only encounter opinions that reinforce their own, limiting critical thinking.

Example: A social media feed that presents only one political viewpoint.

Confirmation bias: The tendency to believe or share information that confirms our existing views, regardless of its truthfulness.

Example: Ignoring credible sources that contradict a favored opinion.

Forms of negative information:

- **Disinformation:** Deliberately false information that is created and spread to deceive or mislead people. *Example:* Fake news designed to manipulate public opinion.
- **Misinformation:** False or inaccurate information that is shared without the intent to mislead. *Example:* Sharing an incorrectly captioned image because the person believes it is true.
- **Malinformation:** Real information used with the intention of causing harm to a person, organization, or country. *Example:* Leaking confidential data to shame someone.
- **Fake news:** Fabricated news presented as legitimate journalism, often spreading through social media. *Example:* Viral headlines claiming fake scientific discoveries.
- **"Deepfake":** Synthetic media (usually video or audio) generated by AI to imitate real people, often in a highly convincing way. *Example:* A video in which words are placed into a politician's mouth.
- **Hate speech:** Speech, writing, or content that attacks a person or group with hatred or incites violence based on race, religion, ethnicity, politics, gender, sexual orientation, or other identity traits. *Example:* "All [ethnic group] people are a threat to us!"
- **Trolling:** Posting deliberately provocative, offensive, or misleading comments online to trigger emotional reactions or start conflicts. *Example:* Commenting on a nature post: "I hope they cut down all the trees!"
- **Clickbait:** Deceptive or overly dramatic headlines designed to make people click—while the content does not deliver what the title promises. *Example:* "You won't BELIEVE what your favorite actor just did!" (And the article reveals it was just a simple interview.)

AI: The good and the not-so-good

“AI is like fire: it can cook your dinner or burn down the house.”



✓ The good stuff AI can do

1. Helps you create cool things

AI tools can help you write, draw, edit videos, or make music.

Example: You give it an idea and it creates art or a short story from it.

It's like having a creative assistant who is always available, day and night.

2. Enhance your learning

AI explains things in different ways (like ChatGPT).

It can help with math, translation, or quizzes to prepare for exams.

It doesn't replace your brain, but it supports it!

3. Makes life more inclusive

Speech-to-text for those who can't type. Tools that describe images for the blind. Translation tools that break down language barriers. Helping people connect, even if they have different needs or languages.

4. Provides protection online

It filters out spam and scam emails.

It monitors for harassment or hate speech on platforms.

It detects fake accounts and suspicious activity.

Some AI works in the background to make the internet safer.

⚠ The not-so-good side of AI

1. Hamis információk terjesztése

Az MI képes deepfake videókat, hamis képeket és hamis hangokat készíteni.

Hamis híreket írhat vagy kitalált tényeket állíthat be úgy, hogy hihetőnek tűnjenek.

Csak mert valami valósnak látszik, még nem biztos, hogy igaz is.

2. Gondolkodás helyettesítése

Ha mindent az MI-re bízol (például hogy írja meg az esszédet), akkor abbahagyod a saját gondolkodást. Így lemaradsz a tanulásról és fejlődésről.

3. Elfogultság beépítve

Az MI az adatokból tanul. Ha az adatok elfogultak (például rasszizmus vagy sztereotípiák), az MI ezt megismételheti. Igazságtalan eredményeket adhat vagy kirekeszthet embereket. Az MI nem tökéletes, azokat tükrözi, akik létrehozták.

4. Követés és adatvédelem

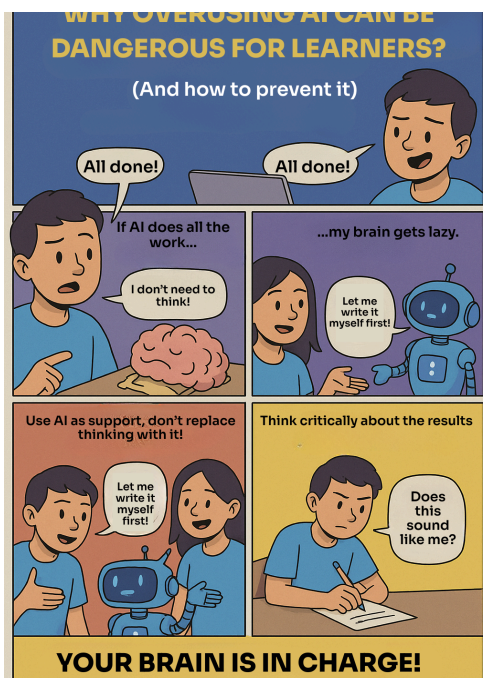
Néhány MI eszköz követi, hogy mit keresel, hogy megismerje a szokásaidat.

Aztán még több hasonló tartalmat mutat — még ha nem is jó neked.

Ezért fontos az alkalmazás beállításait elolvasni és kontrollálni az adataidat.

Why can the overuse of AI be dangerous for students? And how can we prevent it?

“AI is cool. Your mind is even cooler. Use both — but let your brain lead.”



AI is capable of incredible things:

It writes essays
It solves math problems
It explains scientific concepts
It even generates works of art
But here's the thing: if you let it do everything for you, it slowly starts to replace your own thinking — and that's where the danger begins.

What happens if you use AI too much?

1. Your brain gets lazy
2. If AI solves all your problems for you, you don't practice thinking.
3. If you skip training, your muscles get weak — if you don't use your brain, it gets weak too.
4. You lose your own voice
5. AI writes in a clichéd, polite style — but that's not you. Your personality doesn't come through.
6. You learn less, even if you're "ready faster" — but you forget it the next day.

✓ How to use AI wisely (without letting it replace you)

1. Use AI for support, not substitution

Ask it to explain a concept, give examples, or summarize something.
Then use your own words and ideas to write or respond.
Think of AI as a learning partner, not a replacement brain.

2. Start with your own thinking first

Reflect on the task before asking AI for help.
Then compare ideas and strengthen your own.
Don't lose your voice—build on it.

3. Learn to recognize the “AI style”

AI can be useful, but its tone is often too formal or vague.
While writing, always check:
“Does this sound like me?”
“Do I actually agree with this answer?”

4. Keep a healthy balance

Set personal rules:

- ✓ Use AI for reviewing and feedback
 - ✗ Don't let it write full essays for you
- Balance = building your skills + using tools wisely.

Why is learning still important? (Even with AI!)

“Use your brain. Train it. Trust it.”

10 Smart ways to Learn with AI

“AI should expand your mind, not replace it.”

L – Lead with your own thinking.

Begin with your own ideas and reasoning before asking AI for help. AI should build on your thoughts, not replace them.

E – Explore to understand.

Ask AI to clarify, simplify, or illustrate, not to copy answers. Curiosity turns information into knowledge.

A – Ask deeper questions.

Use “why” and “how” questions — not just “what?”. Deeper inquiry builds real understanding.

R – Review and verify.

Be a fact-checker. Compare AI’s suggestions with your notes, books, and trusted sources.

N – Nurture your learning.

Use AI as a coach: ask for practice quizzes, feedback, or study summaries — then reflect on what you’ve learned.

W – Watch your privacy.

Never share personal details, school data, or sensitive information. Learning safely is smart learning.

I – Investigate how AI works.

Understand that AI doesn’t know the truth — it predicts patterns. Knowing this helps you stay critical and in control.

T – Think creatively.

Use AI to brainstorm new ideas or perspectives, but you decide what’s worth keeping.

H – Harness its power responsibly.

AI can support research, writing, and problem-solving — if you use it ethically and purposefully.

A – Apply what you learn.

After using AI, restate key ideas in your own words. If you can explain it clearly, you’ve truly learned it.

I – Inspire others to learn wisely.

Share how AI helped you understand better, not just work faster. Be a role model for responsible, thoughtful learning.

L – Lead with your own thinking

Begin with your own ideas and reasoning before asking AI for help. AI should build on your thoughts, not replace them. Before you ask an AI tool for help, **try to recall what you already know** or sketch out your own answer or plan. This strengthens memory and reasoning — and helps you recognize whether the AI’s reply actually makes sense. Think of the AI as a mirror for your own thoughts — it reflects, questions, and enriches them, but **you remain in charge of the learning process**.

E – Explore to understand

Ask AI to clarify, simplify, or illustrate, not to copy answers.

Curiosity turns information into knowledge.

If something in your textbook or class notes is confusing, ask the AI to:

- explain it in simpler language,
- give an example,
- or show how it connects to other ideas.

✓ This deepens comprehension.

✗ Don’t ask it to *write your essay* — ask it to *help you understand the question*.

A – Ask deeper questions

Use “why” and “how” questions — not just “what?”.

Deeper inquiry builds real understanding.

LLMs are most powerful when you use them as a **thinking partner**.

Ask questions like:

- “Why is this approach better than another?”
- “How can I apply this idea to a real situation?”
- “What might be a counterargument?”

These prompt you to analyse and evaluate — the upper levels of Bloom’s taxonomy.

R – Review and verify

Be a fact-checker. Compare AI’s suggestions with your notes, books, and trusted sources.

Read the AI’s answer critically:

- Does it align with what you’ve learned?
- Can you find evidence for it in reliable sources?
- What would you add or change?

This kind of “cognitive friction” — checking and revising — is where **real learning happens**.

N – Nurture your learning

Use AI as a coach: ask for practice quizzes, feedback, or study summaries — then reflect on what you’ve learned.

AI can be a **tireless tutor**:

- Generate practice quizzes or flashcards.
- Summarize your notes into test questions.
- Ask it to check your reasoning or explain errors.

➡ But always verify correctness — AIs can sound confident even when wrong.

W – Watch your privacy

Never share personal details, school data, or sensitive information.

Learning safely is smart learning.

- Never paste private or school-protected data into an AI tool.
- Always follow your school's academic honesty policy.
- Remember: using AI responsibly shows maturity and builds trust.

I – Investigate how AI works

Understand that AI doesn't *know* the truth — it predicts patterns.

Knowing this helps you stay critical and in control.

You can brainstorm ideas, debate different viewpoints, or draft outlines.

But **you decide which ideas are worth keeping** — that's your intellectual signature.

Understanding that LLMs **predict language patterns, not truth** helps students stay sceptical. Ask:

- "Where did this information come from?"
- "Could there be bias or error here?"

This cultivates **digital literacy** and a scientific mindset.

T – Think creatively

Use AI to brainstorm new ideas or perspectives, but you decide what's worth keeping.

H – Harness its power responsibly

AI can support research, writing, and problem-solving — if you use it ethically and purposefully.

A – Apply what you learn

After using AI, restate key ideas in your own words.

If you can explain it clearly, you've truly learned it.

After every session, ask yourself:

- *What did I actually learn?*
- *What could I now explain without looking it up?*
- *Did this tool make my thinking deeper or just faster?*

Reflection turns information into knowledge.

I – Inspire others to learn wisely

Share how AI helped you understand better, not just work faster.

Be a role model for responsible, thoughtful learning.

■ **Project:** 101132954—DRONE—ERASMUS-EDU-2023-PI-FORWARD

■ Teacher and school leaders training to promote Digital literacy and combat the spread of disinformation among vulnerable groups of

Created by the ELTE DRONE team using ChatGPT 5.0 on October of 2025 (v.2025.10.24):

- Dr. Márta Turcsányi-Szabó, habil associate professor (tszmarta@inf.elte.hu), the Dean's commissioner for educational innovation at ELTE Faculty of Informatics
- Franciska Mikófalvy, ELTE IK T@T Kuckó coordinator

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Copyright information



CC BY-NC 4.0



BY: Credit must be given to you, the creator.



NC: Only noncommercial use of your work is permitted.



Noncommercial means not primarily intended for or directed towards commercial advantage or monetary compensation.

Creative Commons Attribution-Noncommercial 4.0 International

This license requires that re-users give credit to the creator. It allows re-users to distribute, remix, adapt, and build upon the material in any medium or format, for noncommercial purposes only.



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.