

## HANDBOOK FOR YOUTH

### CHAPTER 1: UNDERSTANDING DIGITAL LITERACY

#### WHAT IS DIGITAL LITERACY?

Digital literacy is the ability to access, manage, understand, integrate, communicate, evaluate, and create information safely and appropriately through digital technologies. Here are three expert definitions:

UNESCO (2018). Digital literacy encompasses the ability to navigate digital technologies for



employment, decent jobs and entrepreneurship. It includes competences that are variously referred to as computer literacy, ICT literacy, information literacy and media literacy.

These are the key components of digital literacy:

**Computer literacy.** The knowledge and ability to use computers and related technology efficiently, with skill levels ranging from elementary use to computer programming and advanced problem solving.

**ICT literacy.** Knowing how to use information and communication technology (ICT) to solve problems, manage data, and understand the technical aspects of digital tools. It also involves basic troubleshooting and understanding how to stay secure online

**Information literacy.** Knowing how to search for information, assess its credibility, and use it appropriately. For instance, when doing research for schoolwork, understanding the difference between academic sources and blogs or opinion-based articles.

Media literacy. This involves understanding the impact of media on individuals and society. It means recognizing biases in the news and advertisements, and knowing how to evaluate whether what you see or hear in the media is true or designed to manipulate you.

ITU (2010). Digital literacy consists of equipping people with ICT concepts, methods and skills to enable them to use and exploit ICTs. The related concept of information literacy consists of providing people with concepts and training in order to process data and transform them into information, knowledge and decisions. It includes methods to search and evaluate information, elements of information culture and its ethical aspects, as well as methodological and ethical aspects for communication in the digital world.

European Commission (2016). Digital literacy lays out five digital competence areas and a total of 21 digital competencies. The digital competence areas include information and data literacy, communication and collaboration, digital content creation, safety, and problem-solving.

## WHY IS DIGITAL LITERACY IMPORTANT?

Digital literacy is a crucial skill for navigating today's online world. Here are real-life examples of its importance:

- ★ **Helps you to avoid misinformation and fake news.** Imagine you see a shocking headline about a celebrity scandal. Without checking the facts, you share it - only to find out later that it was fake news! Digital literacy helps you check sources and avoid spreading false information.
- ★ **Protects your personal data and online identity.** A teenager posts a picture of their new apartment on social media with the address visible. Later, they receive unexpected visits from strangers who found the address online. Understanding online privacy helps prevent unwanted attention and potential safety risks.
- ★ **Enables responsible and ethical online behavior.** Cyberbullying and hate speech are serious problems. Digital literacy can help you engage in positive interactions online and recognise when to report harmful content.

- ★ **Empowers you to stay safe from online threats.** Have you ever received an email saying you won a prize, but you never entered a competition? Digital literacy enables you to recognize phishing scams and avoid suspicious links.

## EU POLICIES ON DIGITAL LITERACY AND SAFE SOCIAL MEDIA

The European Union has implemented several policies to ensure that young people can navigate the digital world safely and responsibly. Here are the key policies you should be aware of:

### 1. General Data Protection Regulation (GDPR) Regulation (EU) 2016/679

- Protects your **personal data** and online privacy.
- Gives you the right to **control, delete, and manage** your information on social media.
- More info: <https://gdpr.eu>

### 2. Digital Services Act (DSA)

- The DSA regulates online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms.
- Its main goal is to prevent illegal and harmful activities online and the spread of disinformation.
- It ensures user safety, protects fundamental rights, and creates a fair and open online platform environment.
- Makes platforms **more transparent** about how algorithms work.
- More info:  
[https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en)

### 3. EU Code of Practice on Disinformation

- Helps fight **fake news and misinformation**.
- Encourages platforms to label or remove misleading content.

#### 4. Safer Internet Day (SID)

- A yearly initiative to raise awareness about **cybersecurity and digital responsibility**.

#### Why does this matter to you?

- Helps you **stay safe online** and avoid scams.
- Ensures that **social media companies protect your rights**.
- Gives you tools to **report and remove harmful content**.

## ESSENTIAL DIGITAL LITERACY SKILLS

To stay safe and responsible online, mastering this skills is essential:

1. Fact-checking and media literacy:
  - Always verify information from multiple reliable sources before sharing.
  - Use fact-checking websites like *Snopes* or *Google Fact Check*.
  - Look for credible sources (.gov, .edu, or well-known news outlets).
2. Privacy settings and online security:
  - Adjust privacy settings on social media to control who can see your posts.
  - Use strong passwords and enable two-factor authentication.
  - Understand the concept of “digital footprints” - once something is online, it can be difficult or impossible to remove. Be cautious with what you share.
3. Recognizing scams and phishing attempts:
  - Be cautious of messages asking for personal or financial information.
  - Check URLs before clicking – scammers use fake website links.
  - Don’t download suspicious attachments or respond to unknown emails.
4. Online reputation management:
  - Think before you post – everything online can be permanent.
  - Google yourself regularly to see what information is available about you.

- If you find harmful content about yourself, report or request removal.

### **TEST YOUR DIGITAL LITERACY: 4 QUICK QUESTIONS.**

1. How can you verify if an online news story is true?
  - a. Trust any website that looks professional.
  - b. Check multiple reliable sources.
  - c. Share it quickly before others do.
2. What should you do if you receive a suspicious email?
  - a. Click the link to check if it's real.
  - b. Reply and ask for more details.
  - c. Ignore it and delete it.
3. Why should you be careful about what you post online?
  - a. Employers or schools might check your online presence.
  - b. It disappears after 24 hours.
  - c. Only your close friends can see it.
4. What's a good way to protect your social media accounts?
  - a. Use the same password for all accounts.
  - b. Enable two-factor authentication.
  - c. Share your password with friends for safekeeping.

(Correct answers: 1.b; 2.c; 3.a; 4.b).

### **TIPS TO REMEMBER**

- ★ "Think before you click!"
- ★ "Not everything online is true – check before you trust."
- ★ "Your online posts can follow you forever!"



Co-funded by the  
European Union

[UNESCO Institute for Statistics \(2018\). A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2](#)

[International Telecommunication Union. World Telecommunication/ICT Development Report 2010: Monitoring the WSIS Targets](#)

[European Commission. Education and training glossary. \(accessed 01/2016\)](#)

## CHAPTER 2: DEALING WITH CYBERBULLYING.

### ? WHAT IS CYBERBULLYING?

Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones. It is repeated behaviour, aimed at scaring, angering or shaming those who are targeted.

Digital bullying can take many forms. It might be a one-time incident, but more often than not, it is a continuous pattern of hurtful online behavior. Understanding the signs, effects, and response strategies is crucial for everyone.

Examples include:

- Spreading lies about or posting embarrassing photos or videos of someone on social media.
- Sending hurtful, abusive or threatening messages, images or videos via messaging platforms.
- Impersonating someone and sending mean messages to others on their behalf or through fake accounts.
- Engaging in sexual harassment or bullying using generative AI tools.

Remember that face-to-face bullying and cyberbullying can often happen alongside each other. But cyberbullying leaves a digital footprint – a record that can prove useful and provide evidence to help stop the abuse.

Some common types include:

- **Harassment:** Repeated, hurtful messages that are intended to intimidate or shame the victim. These messages can take the form of insults, threats, or hate speech.
- **Impersonation and Catfishing:** Someone pretends to be another person online to hurt or manipulate others. This might involve creating fake social media profiles or sending messages pretending to be someone else.
- **Trolling and Flaming:** Posting hurtful or offensive comments online to provoke or annoy others. This can happen in comment sections, forums, or social media platforms.
- **Outing:** Revealing private or embarrassing information about someone online without their consent. This can include photos, videos, or personal details.

- **Spamming:** Sending large amounts of unsolicited messages, often for commercial or malicious purposes.
- **Gaslighting:** Psychological manipulation online to make someone doubt their own memory, perception, or reality.

## **WHAT IS THE DIFFERENCE BETWEEN JOKING AND CYBERBULLYING?**


All friends joke around with each other, but sometimes it's hard to tell if someone is just having fun or trying to hurt you, especially online. Sometimes they'll laugh it off with a "just kidding," or "don't take it so seriously."

But if you feel hurt or think others are laughing at you instead of with you, then the joke has gone too far. If it continues even after you've asked the person to stop and you are still feeling upset about it, then this could be bullying.


And when the bullying takes place online, it can result in unwanted attention from a wide range of people including strangers. Wherever it may happen, if you are not happy about it, you should not have to stand for it.

Call it what you will – if you feel bad and it doesn't stop, then it's worth getting help. Stopping cyberbullying is not just about calling out bullies, it's also about recognizing that everyone deserves respect – online and in real life.

## **HOW TO RECOGNIZE CYBERBULLYING AND RESPOND SAFELY**

 Signs of cyberbullying:

- Being targeted by hurtful messages or threats online.
- Seeing hurtful content posted about you without your permission.
- Being excluded or targeted in group chats.
- Fake accounts created to impersonate or embarrass you.

 How to respond:

1. **Don't engage:** Responding may escalate the situation. It's better to report and block the person rather than arguing online.
2. **Take evidence:** Always take screenshots of harmful content to have proof when reporting the bullying.

3. **Report and block:** Use the reporting and blocking tools available on most social media platforms to prevent further harm.
4. **Talk to someone you trust:** It can be difficult to deal with bullying alone. Talking to a parent, teacher, or counselor can help you get support.

## **WHAT ARE THE EFFECTS OF CYBERBULLYING?**

When bullying happens online it can feel as if you're being attacked everywhere, even inside your own home. It can seem like there's no escape. The effects can last a long time and affect a person in many ways:

Mentally, cyberbullying can cause anxiety, depression, and fear. Victims often worry about being targeted again or humiliated publicly. The constant negativity can lead to feelings of hopelessness, sadness, and a diminished sense of self-worth. Additionally, the fear of being attacked online, whether through messages or public posts, can leave a person feeling on edge and scared.

Emotionally, victims may experience shame and guilt, even though the bullying is not their fault. The feeling of being judged or mocked publicly can leave someone embarrassed and emotionally drained. It can also lead to a loss of interest in the things they once enjoyed. The constant attacks can make it hard to focus on hobbies or activities that used to bring joy. Some might also feel incredibly lonely, believing they have no one to turn to for support.

The effects of cyberbullying can also take a physical toll. Stress from being bullied online can lead to sleep problems, making it hard to rest and causing tiredness during the day. Some victims may experience physical symptoms like headaches or stomach aches due to the stress and anxiety. Additionally, eating habits can change; some may overeat to cope, while others may lose their appetite entirely.

Cyberbullying also affects a victim's social life. Victims might withdraw from friends and family to avoid further hurt, leading to isolation. This emotional withdrawal can also damage relationships, causing misunderstandings or arguments. If the bullying is severe, it can lead to a lack of trust in others, making it difficult for victims to build healthy relationships in the future.

In summary, the effects of cyberbullying extend beyond online interactions, affecting the mental, emotional, physical, and social well-being of victims. It's important to be aware of


these effects and offer support to those who are suffering from online bullying, whether by listening, seeking help, or encouraging them to speak up.

## **HOW TO GET HELP**

### **Hotlines & Support Resources:**

#### **National Helplines.**

- Cyprus Helpline 1480 or [1480helpline@cyearn.pi.ac.cy](mailto:1480helpline@cyearn.pi.ac.cy)
- Poland
  - Helpline for children and youth 116 111
  - Helpline for parents and professionals 800 100 100
- Germany Nummer gegen Kummer (Germany)
  - Helpline for Children and Adolescents: 116 111
  - Helpline for Parents: 0800 111 0550

 **Social Media Reporting Tools.** Instagram, TikTok, and Facebook have reporting options. Check them and see how to do it.

- **Facebook/Instagram/Threads**
  - Block or mute people, including new accounts they might create.
  - Limit interactions by hiding comments or message requests from strangers.
  - Use "Restrict" to protect your account without notifying the person.
  - Moderate comments and adjust settings to control who can message you.
- **TikTok**
  - Control who can comment on your videos (friends, everyone, etc.).
  - Filter or delete offensive comments in bulk.
  - Use Comment Care Mode to automatically filter inappropriate comments.
- **X (Twitter)**
  - Choose who can reply to your posts (everyone, people you follow, or people you mention).
  - Mute, block, or report harmful accounts and comments.

- Safety Mode temporarily blocks accounts using harmful language.

**Teachers & School Counselors** – Schools can take action to stop cyberbullying.

 **TEST:** 4 scenario-based questions.

1. What should you do if someone sends you threatening messages online?

Possible answers:

- Do not reply or engage with the person.
- Take screenshots of the messages as evidence.
- Block and report the sender on the platform.
- Inform a trusted adult, teacher, or counselor.
- If the threats are serious, consider reporting to the authorities.

2. A friend is being bullied in a group chat—how can you support them?

Possible answers:

- Reach out to your friend privately and offer support.
- Encourage your friend not to respond to the bully.
- Suggest to report and block the person responsible.
- If comfortable, speak up in the chat and call out the bullying in a respectful way.
- If the situation is serious, tell a teacher, counselor, or a trusted adult.

3. You see someone posting false rumors about a classmate—what's the best response?

Possible answers:

- Do not share, like, or comment on the false information.
- Report the post to the social media platform.
- Privately check in with the classmate to offer support.
- If safe to do so, speak up and say that spreading false rumors is harmful.
- Encourage others to stand against misinformation.

4. How can you report cyberbullying on social media?

Possible answers:

- Use the reporting feature on the platform (e.g., Instagram, TikTok, Facebook).
- Block the person who is bullying.
- Adjust your privacy settings to limit who can interact with you.
- Save screenshots of the harmful content before reporting.
- If the situation continues, seek support from a teacher, counselor, or a trusted adult.

 **REMEMBER!**

"If you wouldn't say it in person, don't say it online!"

"Think before you type – your words have power."

"Support, don't spectate. Stand up against cyberbullying."

 **BIBLIOGRAPHY:**

<https://www.unicef.org/end-violence/how-to-stop-cyberbullying>