CYBER SAFE-Z

Safe Spaces for Gen Z in the Digital World: Training on Combating Cyberbullying

CYBERSAFE-Z | Guidebook

Co-funded by the European Union

Project & Contributors

This guidebook has been developed as part of the “CYBERSAFE-Z: Safe Spaces for Gen Z in the Digital World: Training on Combating Cyberbullying” project.

Project Name:
“Safe Spaces for Gen Z in the Digital World: Training on Combating Cyberbullying”

Project Number:
2025-1-PT02-KA210-YOU-000364874

Publication Date:
05 January 2026

Partners and Contributors:
SYAJ - Associação SYnergia Braga,
projects@synergia.pt

POLIVISION Foundation
fundacjapolivision@gmail.com

VšĮ Švietimas ir paveldas
tasdemirmustafa27@gmail.com

This project has been funded with support from the European Commission. This document 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. Agreement number: 2025-1-PT02-KA210-YOU-000364874

SAFE-Z
CYBER SAFE-Z

Co-funded by the European Union

Acknowledgement

This guidebook has been developed as part of the ERASMUS+ Small Scale Partnership project “Safe Spaces for Gen Z in the Digital World: Training on Combating Cyberbullying” funded by the European Commission under Grant Agreement number 2025-1-PT02-KA210-YOU-000364874. The project has a duration of 12 months, and this publication was released on 05 January 2026.

This project was made possible through the collaborative efforts of our partners:

- SYNERGIA (PT)
- POLIVISION (PL)
- SIP (LT)

Special thanks to the youth workers, participants and facilitators who brought their knowledge, creativity, stories, and perspectives into every module.

CYBER SAFE-Z

Co-funded by the European Union

Contents:

SAFE-Z
CYBER SAFE-Z

Co-funded by the European Union

INTRODUCTION

CYBERSAFE-Z (Safe Spaces for Gen Z in the Digital World: Training on Combating Cyberbullying) is an Erasmus+ KA210-YOU small-scale partnership that supports young people (13–18) and youth workers in recognising, preventing, and responding to cyberbullying while strengthening safer and more resilient digital habits. The project runs for 12 months (01/09/2025–31/08/2026) and is implemented by partner organisations from Portugal, Poland, and Lithuania.
The project is built around a community-centred approach, bringing together youth, youth workers, and educators to create a safer and more supportive online environment. It addresses the Erasmus+ priority of digital transformation through the development of digital readiness, resilience, and capacity, and contributes to improving the quality and innovation of youth work.

Why cyberbullying and digital resilience matter

Cyberbullying can happen across social media, messaging apps, group chats, and online games, and can cause significant emotional and psychological harm. Beyond the immediate online incident, it can affect mental wellbeing, peer relationships, and school engagement. For this reason, young people need both (1) protection skills (digital safety and data protection) and (2) recovery skills (digital resilience and coping strategies). At the same time, youth workers and educators often need practical tools and structured guidance to recognise cyberbullying, intervene appropriately, and support young people effectively.

Who this guidebook is for and what it provides

This guidebook is designed primarily for youth workers, educators, and NGO staff who deliver workshops and learning activities with young people aged 13–18. It can also be used by volunteers and community actors supporting youth digital wellbeing, and selected parts may be used directly with young people as handouts or self-learning pages.

SAFE-Z CYBER SAFE-Z
SYnergia Braga
POLIVISION
Co-funded by the European Union

The guidebook offers practical learning content that supports the project objectives of:

- Empowering young people to recognise, prevent, and respond to cyberbullying;
- Strengthening practical skills related to privacy settings, safe online behaviour, and help-seeking;
- Promoting positive and responsible digital interactions;
- Supporting youth workers with training and ready-to-use educational materials.

How The Guidebook Is Organised

The CYBERSAFE-Z Educational Guidebook is structured as a six-modules. Each module combines short, accessible theory with non-formal education (NFE) activities that can be implemented in youth centres, schools, and community settings. The modules are intended to be flexible: facilitators can deliver them as standalone sessions or as a sequence, depending on local needs and time.

Each module contains:

- A short theory section (definition, key concepts, examples, and facilitator tips)
- At least one ready-to-use NFE activity (step-by-step)
- Evaluation questions (a quick learning check)
- Discussion question(s) (reflection and group dialogue)

Modules in this guidebook:

1. Understanding Cyberbullying and Its Types
2. Digital Security and Data Protection
3. Digital Resilience and Coping Strategies
4. Real-Life Cyberbullying Scenarios
5. Role-Playing and Communication Exercises
6. Support Mechanisms and Reporting Methods

The guidebook is part of a wider package of project activities and outputs, including an online needs analysis (at least 75 young people), three webinars for youth workers (45 participants), nine youth awareness workshops (90 young people), nine cyberbullying scenarios developed with participants, and a peer-support social media campaign featuring nine short reels.

How To Use These Materials In Practice

Facilitators are encouraged to choose the module(s) that best match their group's needs, age, and local digital context. Before starting, create a safe learning environment by agreeing on group rules (respect, no naming individuals, confidentiality limits, and the right to pass). Use the examples as inspiration and adapt them to the platforms and situations young people use locally. Avoid asking participants to share personal trauma publicly; instead, allow optional, anonymous reflections and always offer an opt-out from role-plays or sensitive exercises.

Each session should end with a clear support message: where young people can go if they need help, who they can talk to, and what steps they can take to stay safe (e.g., save evidence, block/mute, report, and contact a trusted adult or support service).

Learning Methods And Accessibility

The guidebook uses a non-formal education approach that is interactive and youth-centred, combining short facilitator input with discussion, case studies, scenario analysis, role-play, and structured reflection. These methods help participants practise decision-making and communication skills, not only learn definitions.
To ensure accessibility across different settings and countries, the materials should be delivered in clear, simple language that can be translated into partner languages. Facilitators should avoid jargon and judgemental labels, focus on behaviours (not "bad people"), and use inclusive examples reflecting diverse backgrounds and experiences, including young people from disadvantaged contexts (e.g., rural areas, migrants, or those with limited access to support).

Resources

To strengthen implementation, facilitators are encouraged to connect the gu content with reliable resources and national support pathways, such as:

- Better Internet for Kids (European portal)
- National Safer Internet Centres (support and reporting guidance)
- UNICEF resources on online safety and wellbeing
- Platform safety centres (e.g., Instagram, TikTok, Snapchat, YouTube, Discord)
- Local child protection, counselling services, school support structures, and helplines

CYBER SAFE-Z
Synergia Braga
POLIVISION
Co-funded by the European Union

CYBER SAFE-Z

Module 1:

Understanding Cyberbullying and Its Types

Co-funded by the European Union

Module 1 - Understanding Cyberbullying and Its Types

Definition

Cyberbullying is a form of bullying that happens through digital technologies such as social media,messaging apps, online games, forums, and group chats.It involves intentional harmful behaviour that targets a person and causes emotional, social, or reputational harm. What makes cyberbullying especially difficult is that it can spread quickly, reach a large audience, and follow a person beyond school or youth spaces. It is helpful to distinguish three situations:

- Online conflict: a disagreement or argument between people of similar power (may be rude,but not always bullying).
- One-time harm: a single hurtful incident (serious, but not necessarily bullying).
- Cyberbullying: harm that is repeated or can be repeated easily (e.g., sharing content), often connected to a power imbalance and ongoing pressure.

Key characteristics of cyberbullying

Cyberbullying often includes some of the following elements (not always all at once):

- Repetition: harmful messages, comments, posts, or actions happen repeatedly, or content is shared/reshared many times.
- Power imbalance: the target has less power (e.g., facing a group, a popular person,
- anonymous accounts, or someone with access to private images/messages).
- Publicness and reach: harmful content can be seen by many people quickly (comments,stories, group chats, reposts).
- Persistence: online content can remain available, be screenshotted, and return later.
- Anonymity and distance: people may bully more easily when they feel hidden or disconnected from the victim's emotions.

Different forms (types) of cyberbullying

Young people may experience cyberbullying in different ways. Common types include:

1. Harassment and insults

Repeated rude, humiliating, or aggressive messages (DMs, group chats, comments).
Examples: name-calling, mocking, threats, spamming someone with hateful content.

2. Public shaming and humiliation

Embarrassing someone in front of others through comments, memes, edits, or "exposing"posts.
Examples: posting screenshots to "prove" something, making a humiliating video,encouraging others to laugh.

3. Exclusion and social isolation

Deliberately leaving someone out of groups, chats, or online activities to punish or controlthem.
Examples: creating a new group chat without someone and posting jokes about it, removing someone repeatedly from a gaming team.

4. Impersonation and fake accounts

Pretending to be someone else to damage their reputation or relationships.
Examples: creating a fake profile using someone's photos, posting "confessions" or rude messages in their name.

5. Spreading rumours and sharing private information

Sharing personal information, secrets, screenshots, or private messages without consent.
Examples: forwarding private photos/messages, sharing someone's address/phone number(doxing).

6. Image-based abuse (including non-consensual sharing)

Sharing or threatening to share images/videos without consent, or using edited/AI-alteredcontent to humiliate.
Examples: sending a private photo to a group chat, creating an edited image to shame someone.

Short examples and typical effects

Below are short, realistic examples and the kinds of effects they may have. (They can be adapted to local platforms.)

Example 1: Group chat attacks: A young person is repeatedly mocked in a class group chat. Others react with laughing emojis and add new insults.
Possible effects: shame, anxiety before school, withdrawal from peers, feeling unsafe, sleep problems.

Example 2: Exclusion in online gaming: Someone is kicked from a team repeatedly and told, "Nobody wants you here."
Possible effects: loss of confidence, isolation, anger, reduced motivation, avoidance of hobbies.

Example 3: Fake account: A fake profile copies a young person's photos and posts embarrassing content pretending it is them.
Possible effects: fear, panic, damaged reputation, mistrust of others, stress about meeting peers offline.

Example 4: Screenshot sharing
Private messages are shared publicly to "prove" a point, and others comment .Possible effects: humiliation, loss of friendships, feeling exposed, reluctance to trust or communicate online.

Example 5: Photo shared without consent
A personal photo is forwarded in a group chat and becomes a joke.
Possible effects: intense embarrassment, fear of judgment, school avoidance, possible trauma response.

Practical tips for youth workers (introducing the topic safely)

Cyberbullying can be sensitive. Youth workers should create a safe learning environment first and avoid increasing harm.

1. Set group rules at the start: respect, no real names, no sharing private screenshots,confidentiality limits, and the right to pass.
2. Use anonymised scenarios: avoid asking participants to share personal stories in the group;offer anonymous or fictional examples.
3. Separate behaviour from identity: focus on actions ("harmful behaviour") rather than labels("bully", "victim") to reduce shame and defensiveness.
4. Acknowledge feelings: name emotions that may come up (anger, fear, embarrassment) and normalise seeking help.
5. Watch for triggering content: avoid graphic or sexualised examples; allow opt-out from role-play or discussions if needed.
6. Be ready with support pathways: have contact details for school counsellors, youth centre support, helplines, or child protection services.
7. Emphasise safe first steps: save evidence, block/mute, report, and tell a trusted adult—repeat these steps clearly.
8. End with a support message: remind participants they are not alone and help is available,including a private conversation after the session if needed.

NFE Activity

Conflict or Cyberbullying? Scenario Sorting

When to use it?

Use in Module 1 right after introducing the definition of cyberbullying and the key criteria(intent, repetition/spread, power imbalance, consent/privacy, audience effect).This activity works especially well as an early "awareness + critical thinking" exercise.

Activity Type

Offline (easy to adapt to online/hybrid with shared slides + breakout rooms)

Target Groups

Young people aged 13–18; Group size: 8–15 (ideal: 10)
Suggested time: 30–45 minutes (including debrief)

Skills Addressed

Recognising cyberbullying and its types; Distinguishing conflict vs bullying vs other online harm; Critical thinking using clear criteria; Upstander mindset (safe support actions)

Materials Needed

Scenario cards (print the ready set below; 10–12 cards)
3 signs or papers: A) Cyberbullying / B) Conflict / C) Not sure / Depends
Flipchart/whiteboard + markers
Sticky notes or small stickers (two colours if possible)
Timer/phone
Optional: projector (to show criteria and scenarios)

CYBER SAFE-Z
Synergia Braga
POLIVISION
Co-funded by the European Union

Description

Participants read short "digital life" scenarios and decide whether each one is cyberbullying, conflict/misunderstanding, or unclear/depends. They must justify their choices using simple criteria: intent, repetition/spread, power imbalance, consent/privacy, and audience effect. The activity ends with a short "upstander micro-practice" so participants leave with practical ways to help.

How to use it?

Step 0 — Prepare before the session (5 minutes, facilitator only)

Print and cut the scenario cards (provided in annex).
Prepare three areas on a wall/board/table:

A) Cyberbullying
B) Conflict / Misunderstanding
C) Not sure / Depends

Write the criteria on a flipchart (or print them):

CYBERBULLYING CRITERIA (simple version):
Intent: Was it meant to hurt or humiliate?
Repetition / Spread: Is it repeated, or can it be shared many times?
Power imbalance: Is someone "outnumbered," exposed, or unable to defend themselves?
Consent / Privacy: Were private messages/photos shared without permission?
Audience effect: Can others see it, react to it, or join in?

Step 1 — Set the safe space (5–7 min)

Say something like:
"We will work with fictional scenarios. No real names, no sharing screenshots from real chats."
"You don't need to share personal experiences. You can always say pass."
"We can disagree respectfully. We focus on behaviour, not labeling people."
"If something brings up a real issue for you, you can speak to me privately afterwards."
(If your organisation has safeguarding procedures, remind participants that confidentiality has limits if someone is in danger.)

How to use it?

Step 2 — Introduce the criteria (8–10 min)

Briefly explain each criterion using 1 sentence. Example script:

Intent: "Sometimes people say 'it's a joke,' but we look at whether it causes harm."
Repetition/Spread: "Online, one post can be shared many times—harm repeats."
Power imbalance: "A group vs one person, anonymous account, or embarrassing content creates power."
Consent/Privacy: "Sharing private messages/photos without permission is a big red flag."
Audience effect: "If others can see and react, it can turn into group pressure."

Step 3 — Group sorting (20–25 min)

Split into small groups of 2–4.
Give each group 4–6 scenario cards (mix types)

Task: place each card into one of the three zones:

A)Cyberbullying
B) Conflict
C) Not sure / depends

For each card, groups must write 1–2 reasons on a sticky note using the criteria.
Example reasons: "public + repeated", "private but shared without consent", "one-time
argument, equal power", etc.

Facilitator role: walk around, encourage use of criteria, and ask:
"Which criterion helped you decide?"
"Could this change if it happened repeatedly?"
"Who has power here?"

Step 4 — Whole-group gallery walk (15–20 min)

Each group places their sorted cards on the wall/board.
Everyone walks around and reads the sticky-note reasons.

How to use it?

Each participant gets:
2 agreement stickers (place where they strongly agree)
1 question-mark sticker (place where they disagree or feel unsure)
(No debating yet—just reading and reacting.)

Step 5 — Facilitated discussion (15–20 min)

Pick 3–4 cards that received the most question marks or disagreement.
Use these guiding questions (use 2–3 per card):
"Which criteria are you using to decide?"
"What would make this clearly bullying?" (e.g., repetition, public sharing, group pressure)
"What impact could this have on the person?"
"What could stop it from escalating?"
Facilitator note: If the group says "it's just a joke," respond with:
"Jokes can still harm. Let's check impact and the audience effect. What happens if it spreads?"

Step 6 — Upstander micro-practice (8–10 min)

Choose two cards that are clearly cyberbullying. In the same small groups, participants write three things:
A supportive private message to the target (1–2 sentences).
One safe bystander action (e.g., report, don't share, check in, ask an adult).
One help channel (trusted adult, youth worker, school counsellor, helpline).
Ask 2–3 groups to share their best examples.

Step 7 — Wrap-up (5 min)

Summarise the key learning:
"Cyberbullying isn't only about one mean comment—repetition/spread and power imbalance matter."
"When unsure, focus on safety and support."
"If it happens: save evidence, block/mute, report, tell a trusted adult."
End with a short support reminder: where participants can go locally for help.

Tips for Learners

You can always choose "Not sure/depends"—then explain what information you'd need.
Use the criteria, not guesses about people's intentions.
If something feels unsafe, focus on support and reporting, not confrontation.
Don't share real screenshots or real names—protect privacy.

Resources

National Safer Internet Centre contacts
School counsellor / psychologist / trusted teacher referral options
Platform reporting & blocking guides (Instagram/TikTok/Snapchat/YouTube/Discord,etc.)
Local youth centre contacts / child protection / counselling services

Evaluation

1. Name two forms of cyberbullying (for example: harassment, exclusion, impersonation, sharing private information, image-based abuse).
2. What is one key difference between online conflict and cyberbullying? (Use at least one criterion:repetition/spread, power imbalance, consent/privacy, audience effect, intent.)
3. Write one safe upstander action you could take if you witness cyberbullying (e.g., supportive private message, reporting, not sharing, asking an adult for help).

Discussion Question

Why do you think some people join in cyberbullying (liking/sharing/commenting) even if they know it can hurt someone?

Annex: Scenario Card Set (12 cards)

Cut these into separate cards. You can adapt platform names to your local context.

1. One-time DM argument: Two friends argue in private messages once. Both say hurtful things and then stop.

Suggested category:
B) Conflict / Misunderstanding
Why: One-time, equal power, private; harmful but not clearly bullying.
If placed in Cyberbullying: Validate feelings, then ask:

"Is it repeated or part of a pattern?"
"Is there power imbalance or public audience?"

Key teaching point: One incident can be serious, but bullying usually involves repetition/pattern.

2. Repeated group chat insults: In a class group chat, several people post laughing emojis and insults every time one student writes anything.

Suggested category: A) Cyberbullying
Why: Repeated + group vs one + public/social pressure + humiliation.
If placed in Conflict: Ask:

3. Screenshot shared to shame: Someone shares a private screenshot of a personal confession to embarrass a peer in a group chat.

Suggested category: A) Cyberbullying (or serious online harm)
Why: Consent/privacy violated + public sharing + humiliation + can spread.
If placed in Conflict: Ask:

"Did the person consent to sharing?"
"Can it be reshared and repeated?"
Key teaching point: Sharing private messages/screenshots without consent is a major
red flag.

4. Fake account impersonation: A fake account uses a student's photos and posts embarrassing"confessions" pretending to be them.

Suggested category: A) Cyberbullying
Why: Clear intent to harm + power imbalance (identity control) + reputation damage + public audience.
If placed in Not sure: Ask:

"What is the fake account doing?"
How would it affect the target if others believe it?

Key teaching point: Impersonation is a strong bullying indicator even if it's "only online."

5. **One-time stranger trash talk in a game: A gamer gets mocked by strangers in a match once; it stops after the match ends.**

Suggested category: C) Not sure / Depends
Why: Could be harassment; but it is one-time, strangers, ends after match; unclear if targeted pattern.
If placed in Cyberbullying: Say:

"It's still harmful. Let's check: is it repeated against the same person or spread outside the match?"
If placed in Conflict: Ask:
"Is there a real relationship/conflict here, or just abuse?"
Key teaching point: Not all harm is bullying; still needs safety responses (mute, report).

6. **Exclusion + celebration: A student is removed from a group chat and others post publicly:"Finally!"**

Suggested category: A) Cyberbullying
Why: Exclusion + public humiliation + group power imbalance; often repeated socially.
If placed in Conflict: Ask:

"Was it a one-time boundary decision, or an intentional humiliation?"
"What's the audience effect of 'finally'?"
Key teaching point: Exclusion becomes bullying when used to punish/control and shame.

7. Rumour spread in comments: People repeatedly comment "I heard you cheated" under someone's posts to damage their reputation.

Suggested category: A) Cyberbullying
Why: Repeated + public + reputation harm + audience joining in.
If placed in Not sure: Ask:

"Is it repeated across posts?"
"Does the target have a realistic way to stop it alone?"
Key teaching point: Public repeated rumours are classic cyberbullying.

8. Private photo forwarded: A personal photo shared in trust is forwarded to others without consent.

Suggested category: A) Cyberbullying
Why: Repeated + public + reputation harm + audience joining in.
If placed in Not sure: Ask:

"Did the person agree to it being shared?"
"What happens if it spreads beyond the group?"
Key teaching point: Consent is central; forwarding private images is serious.

9. Pressure to share passwords: Someone says: "If you're really my friend, give me your password so I can check you're not lying."

Suggested category: C) Not sure / Depends (often coercion or controlling behaviour)
Why: Can be controlling; not always bullying, but can be part of harassment/abuse.
If placed in Conflict: Ask:

"Is there pressure or threat?"
"What would a healthy boundary look like?"
If placed in Cyberbullying: Say:
"It may become bullying if repeated, threatening, or used to control and humiliate."
Key teaching point: This is a digital safety red flag and boundary issue.

10. "It was a joke" meme: A meme is made about a student's appearance. It's reposted by others,and the student asks for it to stop.

Suggested category: A) Cyberbullying
Why: Public humiliation + spread/repetition + ignoring request to stop.
If placed in Conflict: Ask:

"What happens after the person asks it to stop?"
"Does the harm increase due to reposting?"
Key teaching point: "Joke" doesn't cancel harm—impact + spread matters.

11. Threat to leak: A person threatens: "If you don't do what I say, I'll post your private messages."

Suggested category: A) Cyberbullying / coercion
Why: Threats + power imbalance + fear/control; serious risk even if not yet posted.
If placed in Not sure: Ask:

"Is the goal to control through fear?"
"What might the target feel and do?"
Key teaching point: Threats are serious; safety and adult support are needed.

12. Tagging to humiliate: A group tags someone repeatedly in humiliating posts so they get notifications and others join in.

Suggested category:
A) Cyberbullying
Why: Repeated targeting + public audience + harassment via notifications + group effect.
If placed in Conflict: Ask:
"Is this an equal disagreement, or repeated targeting?"
Key teaching point: Repeated tagging is harassment and increases public reach.

CYBER SAFE-Z

Module 2

Digital Security and Data Protection

Co-funded by the European Union

MODULE 2 - Digital Security and Data Protection

Definition

Digital security means protecting your accounts, devices, and personal information so that other people cannot access, misuse, or share it without your permission. Data protection means understanding what counts as personal data (photos, messages, location, contacts, school name,usernames, etc.) and controlling who can see it and what can be done with it.

Digital security is not about being "paranoid." It's about having control. Small habits (better
passwords, privacy settings, safe clicking) reduce many risks, including hacking, harassment, identity
misuse, and unwanted contact.

Key concepts:

1. Strong passwords (or passphrases):
   - A strong password is long and unique. Better than "Password123" is a passphrase like: Sunset!Train!Coffee!River (easy to remember, hard to guess).
   - Avoid: birthdays, pet names, school name, "123456", "qwerty".
   - Best practice: one password per account (especially email and social media).

2. Two-factor authentication (2FA):
   - 2FA adds an extra step to login (a code in an app/SMS). Even if someone learns your password, they still can't enter without the code.Turn on 2FA for: email, social media, messaging apps, and gaming accounts.

3. Privacy settings:
   - Privacy settings control who can see posts/stories, comment, tag, message, add you to groups, or find your profile. They help reduce unwanted contact and prevent strangers from collecting information.

4. Phishing (scam messages and fake links):
   - Phishing is when someone sends a fake message or link that looks real to trick you into giving passwords, codes, or personal data. Phishing often uses panic ("Your account will be deleted") or temptation ("Free followers/skins/prize").

5. Oversharing & digital footprint:

- What you post can be saved, forwarded, screenshots can be taken, and content can return later. Your digital footprint is the trail of information you leave online sometimes without meaning to.

6. Permission and consent:

- Consent means someone agreed. Before sharing someone's photo, screenshot, voice note, or personal info, ask: "Do I have permission?"Sharing without consent can cause harm and can become part of cyberbullying.

Examples of risky vs safe behaviour (practical and realistic)

1. Passwords and accounts
- Risky: using the same password everywhere; sharing passwords with friends/partners; staying logged in on shared devices.
- Safer: using a unique passphrase; turning on 2FA; logging out from shared devices;checking "where you're logged in."

2. Links and messages
- Risky: clicking links from unknown accounts; reacting quickly to messages that create fear; entering login details through a link.
- Safer: checking the sender; verifying through another channel; not clicking unknown links; using official app settings for account recovery.

3. Privacy settings and strangers
- Risky: public profiles with open messages; location visible; accepting unknown followers; being added to unknown group chats.
- Safer: limiting who can message/tag; reviewing followers; turning off location sharing; using "friends-only" features.

4. Posting, tagging, and sharing
- Risky: posting private conflicts publicly; sharing screenshots of arguments; posting others' photos without asking.
- Safer: pausing before posting; asking consent; blurring names/screens; reporting fake accounts.

Practical tips for youth workers (talk about safety without fear-mongering)

- Frame it as empowerment: “These are skills that give you control,” not “the internet is dangerous.”
- Use hands-on practice: settings check, “spot the scam,” password makeover—short and practical beats long lectures.
- Avoid shaming: many risks happen because of trust, pressure, curiosity, or misunderstanding. Keep language neutral.
- Encourage small steps: one stronger password, one privacy change, one habit (“pause before clicking”) is progress.
- Be realistic: young people will keep using social media; focus on harm reduction and support, not banning.
- Protect privacy in the room: never ask participants to show their accounts/messages

publicly. If they adjust settings, they do it privately.

NFE Activity

Digital Safety Challenge Stations

When to use it?

In Module 2 as a practical "learning by doing" session after the short theory input on passwords, 2FA, phishing, privacy settings, and consent.

Activity Type

Offline (station rotation). Can be adapted online using breakout rooms and shared slides.

Target Groups

Young people 13–18; 8–15 participants (ideal: 10); 75–95 minutes (including debrief)

Skills Addressed

Password hygiene; phishing recognition; privacy awareness; safe decision-making; consent and sharing rules

Materials Needed

Printed station cards (provided below) + answer sheets
Pens/markers, flipchart/board
Sticky notes or stickers
Optional: smartphones (participants adjust settings privately, not on screen)
Optional: printed screenshots of privacy settings (for offline groups)

Description

Participants rotate through short "challenge stations." Each station presents a commononline situation (password choice, suspicious message, privacy setting, sharing decision).
Teams choose the safest option and explain why. After rotation, the facilitator reveals a simple best-practice checklist. The activity ends with a personal one-step action plan.

How to use it?

Before the session: set up the room (10–15 min, facilitator only)
Create 4 stations (tables or wall areas).
Place station cards + answer sheet + pens at each station.
Put a timer for rotations (10–12 minutes each).
Prepare a "Best Practice Summary" on flipchart (passwords, 2FA, privacy, phishing,consent

1. Warm-up (5 min)

Ask: "What is one online safety habit you already do?"
Take 3–5 quick answers. (No personal stories required.)

2. Explain the rules (3 min)

Participants work in teams of 2–4.
Every 10–12 minutes, teams rotate to the next station (see details in Annex.)
At each station, teams must write:
their chosen answer, and one reason why it's safest.

3. Station rotation (40–50 min)

Teams complete all stations.

4. Reveal & discuss (15–20 min)

For each station, ask one team to share their answer and reason.
Then share the "best practice" solution (short and clear).

5. Personal action plan (7–10 min)

Each participant writes ONE change they will do today (examples):
enable 2FA on one account
change one weak password to a passphrase
tighten who can message/tag them
stop clicking links from unknown accounts

6. Wrap-up (5 min)

Summarise: "Strong passwords + 2FA + privacy settings + safe clicking + consent"
Remind: if an account is compromised or harassment happens, seek help from a trusted adult/youth worker and use platform recovery/report tools.

CYBER SAFE-Z
Synergia Braga
POLIVISION
Co-funded by the European Union

Tips for Learners

Don't ask anyone to show their phone screen or personal accounts.
Keep examples neutral; no real names, schools, or local gossip.
If someone says they were hacked or harassed, acknowledge and offer private follow-up after the session.
Keep tone practical and positive—celebrate small improvements.

Resources

Better Internet for Kids + National Safer Internet Centre
Platform Help Centres (reporting, blocking, account recovery)
Simple youth-friendly guides on 2FA and password managers
Local school/youth centre support contacts and helplines

Evaluation

1. What are two features of a strong password or passphrase?
2. Name one sign that a message or link might be phishing.
3. What is one privacy setting you can change to reduce unwanted contact online?

Discussion Question

Why do you think young people sometimes ignore online safety risks even when they know the risks—and what would help them choose safer habits?

Annex: Station cards (ready to print)

Station 1 — Password Lab
Task A: Circle the strongest password:

A) Anna2009
B) password123
C) Poland#1
D) Sunset!Train!Coffee!River

Task B: Improve this weak password: "football12"
Write a safer passphrase (long + unique).
Guiding questions: What makes a password hard to guess? Why is "one password for all apps" risky?

CYBER SAFE-Z
Braga
POLIVISION
Co-funded by the European Union

Station 2 — Phishing Detective

You receive: “Your account will be deleted today. Click here to verify now: bit.ly/....”
Task: Mark 3 red flags and write what you should do next.
Guiding questions: How does the message pressure you? How can you check if it’s real without clicking?

Station 3 — Privacy Settings Sprint

A 15-year-old has a public profile and receives unwanted DMs.
Task: Choose the safest settings:
Who can message? (Everyone / Friends / No one)
Who can tag? (Everyone / Friends / Approval required)
Location? (On / Off)
Comments? (Everyone / Friends / Limited)
Guiding questions: Which setting reduces unwanted contact fastest? Why might someone still keep some settings public?

Station 4 — Sharing & Consent
You have a funny screenshot from a private chat where a friend made a mistake.
Task: Decide: Share publicly / Share in a group / Don’t share. Explain why.

Guiding questions: Did you have consent? What could happen if it spreads? How would your friend
feel?

CYBER SAFE-Z

Module 3

Digital Resilience and Coping Strategies

Co-funded by the European Union

MODULE 3: Digital Resilience and Coping Strategies

Definition

Digital resilience is the ability to recognise, manage, and recover from negative online experiences, such as cyberbullying, online hate, or emotional distress. It is not about being unaffected by online harm, but about having the awareness, skills, and support to navigate it in a healthy way. This involves understanding the emotional impact of online interactions and developing both internal coping strategies and external support systems.

Key Concepts

1. Emotional Impact: Negative online experiences can trigger a range of emotions, including anxiety, shame, anger, sadness, and isolation. Recognising and naming these feelings is the first step toward managing them.
2. Healthy Coping: These are strategies that help process emotions and solve problems constructively. Examples include talking to atrusted person, taking a break from devices, engaging in hobbies, or reporting harmful content.
3. Unhealthy Coping: These are strategies that may provide temporary relief but often worsen the situation in the long run. Examples include bottling up feelings, retaliating online, isolating oneself, or engaging in risky behaviours.

Examples of Coping Strategies

1. Helpful:

- Connecting: Talking to a friend, family member, or youth worker about what happened.
- Pausing: Stepping away from the screen to get some perspective.
- Self-Care: Doing something enjoyable and relaxing, like listening to music, going for a walk, or drawing.
- Action-Oriented: Blocking the person, reporting the content, and saving evidence.

2. Unhelpful:

- Revenge: Trying to get back at the person who caused the harm.
- Denial: Pretending that it doesn't hurt or that it's not a big deal.
- Isolation: Withdrawing from friends and family.

NFE Activity

Digital Resilience and Coping Strategies

When to use it?

In Module 3, after discussing digital resilience and the difference between healthy and unhealthy coping strategies.

Activity Type

Offline, individual and group work.

Target Groups

Young people aged 13–18; Group size: 8–15. Suggested time: 45-60 minutes.

Skills Addressed

Emotional self-awareness, problem-solving, help-seeking, building a personal support system.
Sticky notes
"Coping Menu" template (can be pre-drawn or created by participants)

Materials Needed

Large sheets of paper or flipchart paper
Markers and pens
Sticky notes "Coping Menu" template (can be pre-drawn or created by participants)

SAFE-Z CYBER SAFE-Z
SYnergia Braga
POLIVISION
Co-funded by the European Union

How to use it?

Introduction (10 mins): Briefly review the concepts of digital resilience and coping. Ask participants to brainstorm different feelings that can come up from online experiences.

Individual Reflection (15 mins): Give each participant a "Coping Menu" template. Ask them to individually fill in strategies they already use or would like to try.

Group Sharing (15 mins): In small groups, participants share one or two ideas from their menu. This allows them to learn from each other.

Gallery Walk (10 mins): Post the group's ideas on the wall. Allow participants to walk around and add new ideas to their own menus.

Wrap-up (5 mins): Emphasise that everyone's menu will be different and that it's a resource they can use and add to over time.

Tips for Learners

There are no right or wrong answers. Your menu is personal to you.
Think about a range of strategies, from small things that make you feel better to bigger actions.
It's okay to ask for help. Including people in your menu is a sign of strength.

Resources

Local mental health support services and helplines.
School counsellors or trusted teachers.
Online resources about digital wellbeing.

Evaluation

1. Name two healthy coping strategies you can use when you have a negative experience online.
2. Who are two people you could talk to if you were feeling down about something that happened online?
3. What is one action you can take on a social media platform to protect your wellbeing?

Discussion Question

What kind of support do you think is most helpful from friends when someone is going through a tough time online? What about from adults?

CYBER SAFE-Z
SYnergia Braga
POLIVISION
Co-funded by the European Union

CYBER SAFE-Z

Module 4

Real-Life Cyberbullying Scenarios

Co-funded by the European Union

MODULE 4: Real-Life Cyberbullying Scenarios

Definition

This module focuses on using realistic, contextual scenarios to help young people develop practical problem-solving skills and empathy related to cyberbullying. Instead of abstract rules, scenarios allow participants to analyze complex situations, understand different perspectives (target, bystander, bully), and practice making safe and constructive choices.

Key Concepts

1. Problem-Solving: Scenarios provide a safe space to think through the consequences of different actions before facing a real situation.
2. Empathy: By exploring the feelings and perspectives of everyone involved, participants can better understand the impact of cyberbullying.
3. Context Matters: The same action can have different meanings on different platforms (e.g., a comment in a private chat vs. a public post). Scenarios help illustrate these nuances.

Examples Scenarios

- Gaming: A player is repeatedly targeted and verbally abused by teammates in a competitive online game.
- Social Media: A humiliating meme about a student is created and shared across different social media platforms.
- Private Chat: A screenshot of a private conversation is shared without consent, leading to rumors and social exclusion.

Practical Tips for Youth Workers

- Anonymity is Key: Always use fictional names and situations. Never use real examples from the group.
- Trigger Warnings: Be mindful that some scenarios may be upsetting. Give participants a heads-up and the option to sit out an activity.
- Focus on Solutions: The goal is not to dwell on the problem but to brainstorm positive and safe responses.
- Adapt to Your Group: Use platforms and situations that are relevant to the young people you work with.

SAFE-Z CYBER SAFE-Z
SYnergia Braga
POLIVISION
Co-funded by the European Union

NFE Activity

Real-Life Cyberbullying Scenarios

When to use it?
In Module 4, after introducing the value of using scenarios.

Activity Type
Offline, small group discussion.

Target Groups
Young people aged 13–18; Group size: 8-15. Suggested time: 50-60 minutes.

Skills Addressed
Critical thinking, empathy, decision-making, identifying safe and unsafe behaviors.

Materials Needed
Printed scenario cards (3-4 different scenarios)
Flipchart paper and markers for each group
Guiding questions for analysis (see below)

Description
In small groups, participants read and analyze a cyberbullying scenario. They discuss the risks, consequences, and potential safe reactions for everyone involved.

How to use it?
Setup (5 mins): Divide participants into small groups and give each group a different scenario card.

Group Analysis (20 mins): Each group discusses their scenario using the following guiding questions: – What is happening in this situation? – Who is involved and what are their roles? – What are the potential risks and consequences? – What is one safe thing the target could do? – What is one safe thing a bystander could do?

SAFE-Z CYBER SAFE-Z
SYnergia Braga
POLIVISION
Co-funded by the European Union

How to use it?

Group Presentations (15 mins): Each group briefly presents their scenario and their key discussion points.

Whole Group Discussion (10 mins): The facilitator leads a discussion comparing the different scenarios and highlighting common themes.

Wrap-up (5 mins): Summarize the key learnings and remind participants of the available support systems.

Tips for Learners

There can be more than one "right" answer.
Think about the situation from all perspectives.
Focus on what you can do to make the situation safer.

Resources

A collection of pre-written, age-appropriate scenarios.
Platform-specific safety guides (e.g., how to report content on TikTok, Instagram, etc.).

Evaluation

1. In the scenario you discussed, what was one safe choice a person could make?
2. Why is it important to think about the perspective of a bystander in a cyberbullying situation?
3. Describe one way you could adapt a scenario to make it more relevant to your own experiences.

Discussion Question

How are the challenges of cyberbullying different in a gaming environment compared to a social media app? What stays the same?

CYBER SAFE-Z

Module 5

Non-Formal Education (NFE) Activity

Co-funded by the European Union

Non-Formal Education (NFE) Activity

Definition:

Role-play is an active learning technique in which participants take on characters or viewpoints to rehearse real-world situations in a controlled, fictional setting. In the context of cyberbullying and online safety, role-play helps young people practise empathising with others, recognise different roles in harmful interactions, and try out supportive communication and safety strategies without personal risk. It is especially effective for building social skills because it combines emotional engagement with practical rehearsal.

Key concepts:

1. Fictional safety: Always use invented scenarios and names to prevent re-traumatisation. No real personal stories should be reenacted.
2. Perspective-taking: Role-play asks participants to temporarily inhabit another person's viewpoint (target, bystander, bully, trusted adult) to deepen empathy and understanding.
3. Behaviour focus: Encourage attention to what people say and do (language, tone,actions), not why someone is a certain way. This keeps feedback practical and non-judgemental.
4. Skill rehearsal: Role-plays are practice space for concrete communication techniques (validation, boundary-setting, reporting, de-escalation).
5. Debriefing: A structured reflection after each role-play that consolidates learning, manages emotions and plans next steps.

Roles:

1. Target (victim): The person experiencing the harmful behaviour. Role-players practise naming feelings, asking for help and setting boundaries.
2. Bystander: Observers who can either ignore, escalate or support. The aim is to practice upstander behaviours: checking in, offering support, and safely intervening online.
3. Bully: The person creating harm or excluding others. In role-play, this role helps identify triggers, common tactics, and how to respond without escalating.Emphasise that playing the bully is not endorsement of behaviour, it is a learning tool.
4. Trusted adult: A parent, teacher, counsellor or youth worker who can be approached for help. Practice includes how to report, what information to give, and how adults can respond supportively.

Communication skills to practise:

1. Validation: Acknowledge feelings (e.g.;That sounds upsetting, I can see why you'd feel hurt).
2. Open, non-leading questions: Encourage sharing (e.g.;Can you tell me what happened?; rather than;Did they do X?.
3. Boundary sentences: Short, clear limits (e.g.;Please do not tag me in posts like that, it makes me uncomfortable;).
4. Safe offers of help: Concrete next steps (e.g. "Do you want me to screenshot and report this with you?.
5. De-escalation phrases: Calm, neutral language to reduce heat (e.g. ;Let's pause here and talk calmly)
6. Reporting language: How to present facts succinctly (what happened, who was involved, where and when).

Examples of brief conversations:

1. Supportive bystander → target

Bystander: "Hey, I saw those comments earlier. That must have felt awful. Are you okay? Do you want me to stay with you while we report it?"
Target: "Thanks. I don't want it to get worse. Can you help me take screenshots?"
Bystander: "Yes, I'll stay and help. We can also send it to a teacher together."

2. Reporting to a trusted adult

Young person: "I need to tell you about something that happened on Instagram. Someone created a group where they shared edited photos of me and called me names. It happened yesterday evening and I have screenshots."
Trusted adult: "Thank you for telling me. You did the right thing. Let's look at the screenshots together and decide whether to report and block."

3. Setting boundaries

Young person to peer: "Please don't tag me in that chat, it makes me uncomfortable when people post my photos without asking. If it happens again I'll have to block the chat."
Peer: "Sorry, I didn't realise. I won't tag you again."

Running role-plays safely (practical tips for facilitators):

1. Pre-brief: Explain aims, reassure that scenarios are fictional, and outline opt-out procedures. Give a trigger warning at the start.

2. Roles and alternatives: Offer alternatives to playing sensitive roles (e.g. observer, note-taker, facilitator assistant, script reader). Rotate roles if appropriate.

3. Small groups: Keep groups to 3–5 participants to minimise exposure and ensure everyone can participate.

4. Time limits: Keep role-plays short (2–5 minutes) and use a timer.

5. Grounding tools: Teach quick grounding techniques (deep breaths, leave the room, 5-4-3-2-1 sensory check) and allow breaks.

6. Emotional safety: Have a private signal (card, hand gesture) participants can use to stop a role-play immediately.

7. Clear boundaries: Remind participants not to use real names or personal details.

8. Active facilitation: Circulate, watch for distress, and be ready to pause or stop a scene.

9. Signposting: Before finishing, remind participants of support resources (counsellor, helpline, Safer Internet contacts).

Allowing opt-out and offering roles:

1. Explicitly state that opting out is respected and not penalised.

2. Provide three safe alternatives: "observer with feedback", "script reader (reads lines only)", or "changer (rewrites the dialogue)".

3. If someone opts out, assign them a constructive task (e.g. note patterns of language, suggest supportive phrases) so they stay engaged without emotional exposure.

Debriefing (immediately after each scene using a calm, structured approach):

1. Check-in (emotions): "How is everyone feeling right now?" Give 30–60 seconds for silent breathing before sharing.
2. Descriptive feedback: Ask what happened (facts, not judgements). "What did you notice?"
3. Impact reflection: "What effect did that behaviour have on the target?"
4. Skill focus: "Which phrases or actions helped? Which didn't?"
5. Action planning: "If this happened for real, what would we do next? Who could we tell?"
6. Support check: Offer one-to-one space for anyone who needs it and restate reporting routes.

NFE Activity

"Walk in My Digital Shoes" – Role-Play for Supportive Communication

When to use it?

Use this activity after introducing core concepts of cyberbullying roles (target, bystander, bully, trusted adult) and basic communication strategies. Ideal as the main practice activity of Module 5

Activity Type

Offline (adaptable to hybrid).

Target Groups

Young people aged 13–20; groups of 8–25 participants.

Skills Addressed

Empathy and perspective-taking
Supportive communication
Upstander behaviour
Recognising unsafe digital interactions
Asking for help and setting boundaries

Materials Needed

3–4 short printed fictional scenarios
Role cards (target, bully, bystander, trusted adult)
Chairs for small groups
Post-its and markers
Timer

Description

Participants act out a short cyberbullying scenario from different perspectives and practice supportive communication, healthy boundaries, and upstander behaviour. The goal is to help youth understand emotional impacts, recognise safer responses, and rehearse practical communication strategies they can use online.

SAFE-Z CYBER SAFE-Z
SYnergia Braga
POLIVISION
Co-funded by the European Union

How to use it?

Introduction (5 min)
Facilitator explains the four roles and the aim of the exercise.
Clarify that real personal stories are used.

Group Division (5 min)
Participants form groups of 4 and receive:
One scenario
Four role cards

Round 1 – Role-Play "Unhelpful Reaction" (10 min)
Groups act out the scenario in a way that shows what not to do (e.g. Ignoring, blaming, escalating).
This helps surface common mistakes.

Round 2 – Role-Play "Supportive Communication" (10 min)
Same scenario, but participants apply supportive behaviours:
Validating feelings
Showing empathy
Using conflict-de-escalating sentences
Suggesting reporting or help-seeking
Etting boundaries

Group Sharing (10 min)
Each group shares:
What changed from Round 1 to Round 2?
What reactions were most effective?

Reflection (5 min)
Participants answer:
Which role was hardest and why?"

Tips for Learners

You may opt out or switch roles at any time.
Use fictional names only.
Focus on behaviours, not blaming.
Avoid reenacting real traumatic situations.
Take a short break if emotions arise.

Resources

Instagram, TikTok, Discord safety centres
National Safer Internet Helpline
School counsellor or local youth workers
EU Better Internet for Kids (BIK) platform

CYBER SAFE-Z
Synergia Braga
POLIVISION
Co-funded by the European Union

Evaluation

1. What is one new thing you learned about cyberbullying roles (target, bystander, bully, trusted adult)?
2. Which supportive phrase or action do you feel most confident using online after this activity?
3. If you saw cyberbullying tomorrow, what is one thing you could realistically do?

Discussion Question

How did it feel to play your role (target, bystander, bully, trusted adult)?
What would you do the same or differently in real life, and why?

CYBER SAFE-Z

Module 6

Support Mechanisms and Reporting Methods

Co-funded by the European Union

Module 6-Non-Formal Education (NFE) Activity

Definition:

Informal support refers to the people and networks young people turn to first: friends, family members, peers, partners and community contacts. These are trusted relationships that offer emotional comfort, practical help and immediate presence. Informal supporters are often the quickest route to feeling understood and safe.

Formal support includes professionals and services with a duty to help and specific tools or powers to act: teachers, school counsellors, youth workers, social services, helplines, the police, and platform moderation teams. Formal supports offer structured assistance: advice, record-keeping, safeguarding measures, referrals and, where needed, statutory intervention.

Key Concepts:

1. Accessibility: Consider who is easy to reach in a crisis (time, language, mobility, online access). Maps should list both in-person and remote options.

2. Confidentiality: Explain the limits of confidentiality for each support (e.g. counsellors may need to report risk of harm).

3. Practicality: Include what each support can actually do: listen, collect evidence, report to platforms, contact families, or escalate to services.

4. Redundancy: Encourage multiple options, a report path with backups if the first option is unavailable.

5. Agency: Support maps should centre the young person's choices, letting them decide who to contact and when.

Examples of support types (short scenarios):

1. Friend (informal): A peer sees insulting memes about a classmate and messages them privately: "I saw those posts, are you okay? Do you want me to help report them?" This is immediate emotional support and can lead to joint reporting.

2. School counsellor (formal): A young person brings screenshots and the counsellor documents the incident, advises on safeguarding steps, and helps contact parents or report to the platform.

3. Helpline (formal/remote): A young person calls a national child helpline late at night to get anonymous advice on blocking and reporting and to hear coping strategies.

Platform Reporting Tools:

1. What to report: Most platforms allow reporting for harassment, hate speech, explicit images, impersonation, doxxing and threats. Teach young people to identify the correct category.

2. How to report: Typical steps are: locate the offending post or account → open the menu (three dots/ellipsis) → choose 'Report' → select reason and attach evidence (screenshots, links) → submit. Some platforms let you block or mute the account at the same time.

3. What happens after reporting: Moderation varies as immediate removal, review queues, warnings, temporary suspensions, or no action if guidelines are not breached. Encourage keeping records (screenshots, timestamps, URLs) and following up if needed.

4. Using in-platform safety settings: Show how to use privacy settings, two-factor authentication, blocking, muting, comment controls and restricted lists to reduce exposure.

Safe Reporting Practices:

1. Gather evidence safely: Take screenshots, copy links and note dates/times. Do not forward abusive content to others unless necessary and with consent. Use private messaging to coordinate reporting with a trusted adult or friend.

2. Protect privacy: Blur personal details if sharing screenshots with a third party for support. Avoid re-sharing abusive posts publicly, this can amplify harm.

3. Report and block: Whenever possible, block the abuser after reporting to stop further contact.

4. Use trusted adults for escalation: If a platform response is slow or the abuse is serious (threats, sexual images, doxxing), involve a trusted adult or professional immediately.

5. Follow up: If no action is taken, escalate through platform appeals or local services; keep a record of all steps.

Tips for Youth Workers (mapping local support and encouraging help-seeking):

1. Start with a community scan: List formal services (schools, youth centres, helplines, health services, police contact points) and informal supports (youth groups, peer mentors). Note opening hours, languages, contact methods and whether they accept anonymous contacts.

2. Build a visual, localised resource bank: Create laminated one-page maps for the youth centre and printable A4 sheets for participants with icons and short contact instructions.

3. Make it youth-friendly: Use clear language, icons and step-by-step mini guides for reporting on popular platforms in your area. Offer QR codes linking to platform safety pages.

4. Run practical demos: Show reporting menus on smartphones or screenshots; practice a mock report in a supervised setting.

5. Normalize help-seeking: Share short stories (fictional or anonymised) showing positive outcomes from seeking help. Reinforce that asking for support is a strength.

6. Train frontline staff: Ensure reception, teachers and youth workers know local reporting protocols and their safeguarding responsibilities.

7. Create backup plans: Encourage each young person to identify at least two trusted contacts and one formal service they can approach.

8. Lower barriers: Offer private sign-up sheets, anonymous reporting boxes, or digital forms so that young people with low confidence can reach out without speaking in public.

9. Follow up: After an incident, check in with the young person and adjust the map if needed.

NFE Activity

"My Digital Support Map & Reporting Pathways"

When to use it?

Use this activity after explaining formal and informal support systems, and after introducing how reporting tools on platforms work.

Activity Type

Offline (with optional online component).

Target Groups

Youth aged 12–20; groups of 10–30 participants

Skills Addressed

Help-seeking
Identifying trusted support
Understanding reporting processes
Digital safety decision-making
Community awareness

Materials Needed

A4 sheets (one per participant)
Colour markers
Printed icons (friends, family, teachers, youth workers, helplines, platform tools)
Smartphones (optional, for exploring reporting menus)
Flipchart

Description

Participants identify all the support options available to them — both online and offline — and learn how to create a clear, safe reporting plan they can use in real situations. This helps reduce barriers to asking for help and increases confidence in effective reporting.

CYBER SAFE-Z
SYnergia Braga
POLIVISION
Co-funded by the European Union

How to use it?

Warm-Up Brainstorm (5 min)
Ask: "Who can you talk to if something online makes you feel unsafe?"
Write categories on a flipchart: Friends, Family, School, Youth Workers, Platforms, Helplines.

Creating the Support Map (10 min)
Participants draw themselves in the centre of the page and place their support options around them using words, icons, or drawings.

Building a Reporting Pathway (10 min)
Participants choose one platform they use (TikTok, Instagram, WhatsApp, Discord) and outline:
Now to block
Now to mute
Where to report
Who to talk to offline after reporting

Pair or Small Group Sharing (5 min)
Participants compare maps and notice differences in the support systems available.

Collective Reflection (5 min)
Discuss: "What stops young people from asking for help, and how can we reduce these barriers?"

Tips for Learners

Support can come from more than one place — you're not alone.
It's okay not to remember all reporting steps; your map helps you keep track.
Screenshots are useful before reporting.
You can contact more than one support person if needed.

Resources

Meta Safety Center (Instagram/Facebook)
TikTok Safety Center
Discord Trust & Safety Hub
National Child Helpline / Safer Internet Hotline
Local youth centres and school counsellors

SAFE-Z CYBER SAFE-Z
SYnergia Braga
POLIVISION
Co-funded by the European Union

Evaluation

1. Who are two people or services you could contact if something online made you feel unsafe?
2. How would you report an abusive post on a platform you use? List the main steps
3. Why is it important to keep evidence (screenshots, times, links) when reporting?

Discussion Question

What stops young people in your community from asking for help when they need it, and what one change could we make to make help-seeking easier?

CYBER SAFE-Z

-Guidebook-

Stay tuned!

Stay connected for more resources and updates on future initiatives. Visit our organisation's websites.

https://www.synergia.pt/
https://polivisionfoundation.pl/
https://svietimasirpaveldas.lt/

Co-funded by the European Union