Co-funded by
the European Union

EthiTech Toolkit

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

ABOUT THE PROJECT

2023-3-NL02-KA210-YOU-000178752

EthiTech is an innovative initiative designed to strengthen youth workers' digital competencies and help them engage young people safely, creatively, and effectively in the digital world. The project addresses growing gaps in digital literacy by providing practical tools that support ethical online behavior, critical thinking, and digital resilience.

The core output of the project is the EthiTech Toolkit—a user-friendly, accessible collection of guides, templates, and best practices covering digital skills, online safety, privacy, digital creativity, information verification, and digital citizenship. The toolkit is co-created by project partners and digital youth work experts, and continuously improved through needs assessments, training sessions, and pilot activities.

By equipping youth workers with clear methods and ready-to-use materials, EthiTech enhances the quality of youth work and supports young people in becoming confident, responsible, and active digital citizens. The toolkit will be available in English and translated into partner languages to ensure broad accessibility and long-term impact.

Jugendvision e.V

YCDA

YOUTH WITHOUT BARRIERS

TABLE OF CONTENTS

01

Introduction

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

The EthiTech Toolkit is a comprehensive educational curriculum designed to address the growing "Digital Skills Gap" and promote social and economic inclusion for young people—especially those from disadvantaged backgrounds, refugee communities, and migrant populations. In a world where digital competence has become the foundation of active participation in society, EthiTech goes beyond basic digital literacy to explore the ethical, psychological, and technical complexities of the modern "Attention Economy."

The toolkit aims to transform young people from passive consumers of digital content into resilient, informed, and active digital co-creators. By adopting a "train-the-trainer" approach, EthiTech equips youth workers with advanced strategies and practical tools that create a ripple effect, empowering marginalized youth to navigate the digital world with confidence, safety, and entrepreneurial potential. The curriculum is built on three interconnected pillars, each addressing a critical dimension of digital life:

1. Building the Digital Self & Resilience

EthiTech challenges the outdated belief that online and offline identities are separate. It introduces the concept of the "Digital Self", emphasizing that digital actions carry real-world consequences. This pillar explores the psychological dynamics of online behavior, including:

Online Disinhibition Effect (benign vs. toxic)

Pluralistic Ignorance and its role in fueling harmful online behavior

The impact of dopamine loops, compulsive scrolling, and algorithmic reinforcement

The formation of filter bubbles and their influence on perception

To support ethical and mindful digital engagement, the toolkit provides practical frameworks such as:

The S3 Model (Safe, Savvy, Social)

The THINK Method (True, Helpful, Inspiring, Necessary, Kind)

This pillar also focuses on digital well-being, teaching young people how to "retrain" algorithms to support their mental health rather than exploit their attention.

2. Navigating Information Disorder & Digital Security

In an era shaped by deepfakes, misinformation, and algorithmic polarization, EthiTech trains learners to become "digital detectives." Instead of relying on vague warnings about "fake news," the toolkit introduces the precise Information Disorder Framework, distinguishing between:

Misinformation – false information shared without harmful intent

Disinformation – intentionally deceptive content designed to cause harm

Malinformation – the use of truthful information to inflict damage

Learners develop strong verification skills through:

The SIFT Method (Stop, Investigate, Find, Trace)

Lateral Reading techniques

This pillar also strengthens technical resilience by clarifying the difference between:

Online Privacy – control over personal data

Online Security – protection against threats and attacks

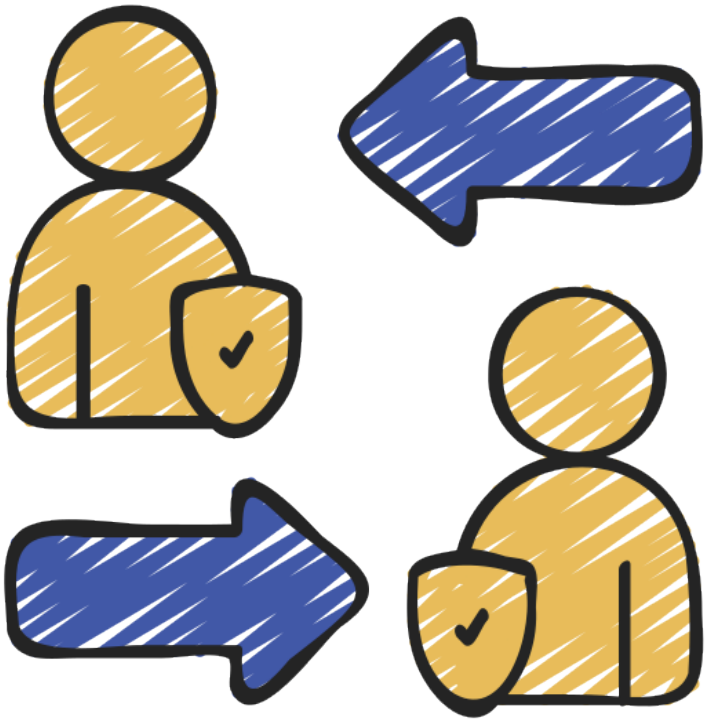
Key topics include:

Social engineering and manipulation tactics

Multi-Factor Authentication (MFA)

Password management

Understanding and managing Passive Digital Footprints



3. Empowering Creativity & Active Digital Citizenship

EthiTech positions technology as a tool for social justice, creativity, and employability. This pillar encourages young people to use digital tools not only for consumption but for meaningful creation.

Key components include:

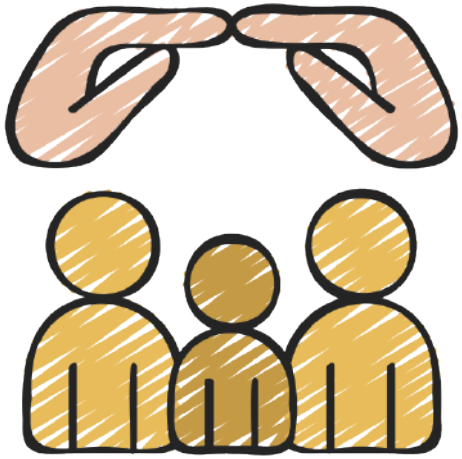
Entrepreneurial Creativity: using digital tools to produce valuable, portfolio-building content

Digital Storytelling: enabling marginalized youth to reclaim their narratives and advocate for their rights

Ethical content creation: informed consent, de-identification, and "Do No Harm" principles

Upstander Culture: applying the 5Ds of Bystander Intervention (Distract, Delegate, Document, Delay, Direct) to address online harassment

The goal is to cultivate a generation of digital citizens who are technically skilled, ethically grounded, and socially responsible.



Learning Outcomes

By engaging with the EthiTech Toolkit, both learners and facilitators will develop competencies across three domains: Theory, Practice, and Ethics.

A. Theoretical Knowledge & Critical Understanding

Participants will be able to:

Define Digital Citizenship and understand its nine core elements (e.g., Digital Law, Commerce, Etiquette)

Analyze the Information Disorder framework (misinformation, disinformation, malinformation)

Understand how the Attention Economy, algorithms, and feedback loops shape online behavior

Recognize psychological triggers such as the Online Disinhibition Effect, dopamine loops, and the bystander effect

Distinguish between Online Security and Online Privacy, including rights under GDPR and CCPA

B. Practical & Technical Skills

Participants will learn to:

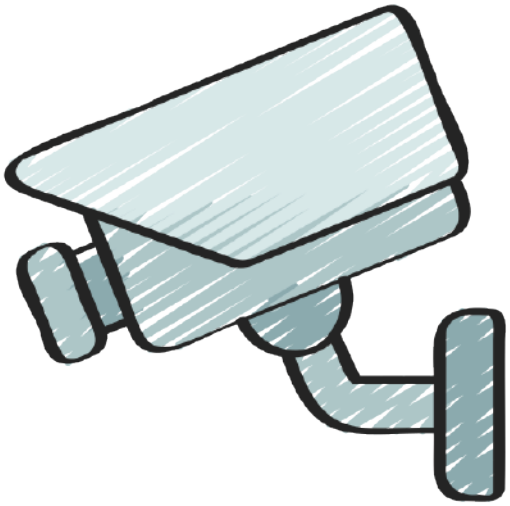
Apply the SIFT Method for fact-checking and source verification

Strengthen digital hygiene through password managers, MFA, and digital safety audits

Manage Active and Passive Digital Footprints, using defensive and offensive strategies

Demonstrate functional competence in information literacy, secure communication, and content creation

C. Ethical & Social-Emotional Competencies



Participants will be able to:

Apply the THINK Method to ensure ethical online communication

Act as Upstanders using the 5Ds of Bystander Intervention

Use Digital Storytelling to express identity and advocate responsibly

Develop Digital Empathy, aligning online behavior with real-world values

Target Audience

The EthiTech Toolkit is designed for a diverse audience, beginning with the primary users—facilitators and educators who directly deliver digital literacy content. This group includes youth workers and trainers in non-formal education settings, educators with limited digital experience who require structured guidance, and NGO staff working in youth development and digital literacy. The toolkit equips them with practical tools, templates, and clear methodologies that strengthen their confidence and capacity to teach digital citizenship effectively.

Beyond the facilitators, the toolkit's primary beneficiaries are young people, particularly those aged 16–25 (and up to 30 in some partner contexts). It supports digital natives who actively use the internet but may lack critical thinking and safety skills, as well as migrants and refugees seeking digital inclusion and communication opportunities. The toolkit also addresses the needs of youth from disadvantaged or rural areas and young people at risk of exclusion due to limited access to digital resources.

Finally, the EthiTech Toolkit benefits a broader secondary audience of stakeholders and communities who play an essential role in shaping young people's digital environments. This includes educational institutions integrating digital literacy into their curricula, policymakers developing youth and digital education strategies, and local communities—parents, families, and caregivers—who support young people's digital well-being. Together, these groups form the ecosystem that enables EthiTech to create lasting impact.

02

Digital Skills and Competencies

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

Basic Functional Skills for Digital Youth Work

This module focuses on the essential digital competencies required for effective, inclusive, and secure youth work. It covers three core areas of the European Digital Competence Framework (DigComp): Information and Data Literacy, Communication and Collaboration, and Digital Content Creation. Together, these skills form the foundation of meaningful youth engagement in the digital age.

A. Theoretical Explanation: Functional Digital Skills and the Inclusion Imperative

Digital skills are no longer optional—they are the foundation of active participation in modern society. For youth workers, functional digital skills serve as a bridge to social and economic inclusion, especially for young people facing structural disadvantages. These skills represent the practical, everyday abilities required to navigate digital environments safely, confidently, and productively.

A1. The Core Competencies (DigComp Focus)

Competency Area	Essential Actions for Youth Workers	Inclusion Relevance (Why it Matters)
Information and Data Literacy	**Searching & Filtering:** Efficiently finding credible, relevant resources. **Evaluating:** Assessing the reliability of sources (e.g., distinguishing fact from opinion/misinformation).	Enables youth to access quality resources for learning, career development, and civic engagement, overcoming the challenge of information overload.
Communication and Collaboration	**Interacting:** Using various tools (email, chat, video) appropriately. **Sharing:** Securely sharing files and data. **Collaborating:** Co-creating documents and running productive online meetings.	Fosters a sense of community and participation, especially for youth who may be geographically isolated or hesitant to speak up in physical settings.
Digital Content Creation	**Developing:** Creating simple digital materials (flyers, presentations, quizzes). **Integrating:** Adapting existing content (e.g., converting a worksheet into an interactive online quiz). **Copyright:** Understanding basic legal use of images/texts.	Allows youth workers to localize, diversify, and personalize content, making it relevant and engaging for young people with diverse learning needs and cultural backgrounds.

A2. The Digital Skills Gap: A Project Mandate

The EthiTech project directly responds to the growing digital skills gap among young people—particularly those from disadvantaged areas, refugee and migrant communities, or low-income backgrounds.

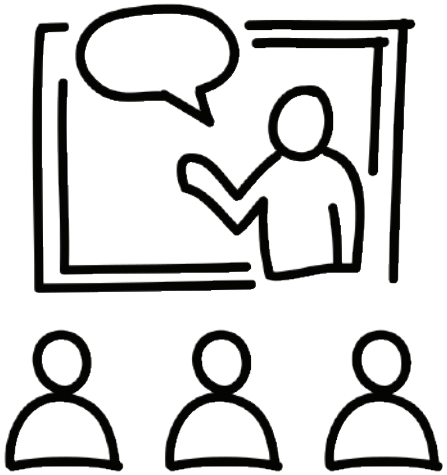
Evidence of Need:

Studies across partner countries show that despite high internet usage, many young people lack essential competencies for employment and critical digital engagement.

Initiatives such as UNDP Türkiye's Digital Youth Centers highlight the urgent need for functional skills like digital communication and basic tool use.

Academic research consistently identifies digital literacy as a key factor in employability and social inclusion.

By training youth workers in these core functional skills, EthiTech creates a multiplier effect—ensuring that marginalized youth gain the competencies needed to participate confidently in the digital public sphere and the labor market.



B. Theoretical Explanation: Functional Digital Skills and the Inclusion Imperative

A Digital Youth Work Hub (DYWH) is the central system where youth workers manage projects, resources, communication, and collaboration. A well-structured and secure hub increases efficiency, accessibility, and safety.

Step	Detailed Action Plan	Key Technical Tips
Platform Selection & Setup	Choose a single, recognized cloud suite (e.g., Google Workspace, Microsoft 365, or a robust open-source LMS). Prioritize consistency—using too many tools creates confusion.	Ensure the platform supports Multi-Factor Authentication (MFA) for your account. Verify accessibility features for users with visual/motor impairments.
Structuring Information & Resources	Create a clear hierarchy: 1. Public (View Only) for general info; 2. Team (Internal) for documents; 3. Collaborative (Editing) for joint activities. Use a consistent tagging or naming system (e.g., [ET_M1_Quiz_V1]).	Use the platform's search function efficiently. Use Version History to prevent loss of work—a key skill for collaborative content creation.
Mastering Sharing & Permissions	Crucial Step: When sharing links, always default to "Restricted" and manually add the specific emails of youth/partners with the minimum necessary permission (Viewer, Commenter, Editor). Never use "Anyone with the link can edit" for sensitive or master documents.	Regularly audit your shared files (e.g., monthly) to ensure no public links were accidentally created. This minimizes data risk (Safety, Module 2).
Content Creation: Presentation Basics	Learn to create a simple, visually appealing resource (e.g., a five-slide presentation on online etiquette). Focus on clear fonts, high contrast, and minimal text to be effective on mobile devices.	Master two features: Export to PDF (for stable sharing) and Embed Link (to share a live presentation on your website or social media).
Facilitating Effective Online Sessions	Prepare an agenda with clear time slots for presentations, discussion, and practical exercises. Use the first five minutes for technical checks (audio/video). Use the "breakout room" feature for small-group discussions to maximize engagement.	Record sessions only with explicit consent and inform participants where the recording will be stored (in the DYWH, with restricted access). Use the Polls or Reactions features for quick engagement checks.

C. Real-Life Example: Enhancing Youth Employability through Digital Portfolios

Project Goal:
Support disadvantaged youth (16–30) in showcasing their non-formal skills through digital portfolios.

Challenge:
Many young people lack professional digital communication skills and struggle to organize their achievements into a shareable format.

Solution:
A structured Portfolio-Building Workshop.

Digital Content Creation

Youth Worker Action:
Provide a mobile-friendly Canva template and teach basic editing.

Outcome:
Youth create professional digital assets without needing advanced software.

Information & Data Literacy

Youth Worker Action:
Share three portfolio examples (excellent, average, flawed) and facilitate group evaluation using a collaborative tool.

Outcome:
Youth learn to critically assess digital content and understand quality standards.

Communication & Collaboration

Youth Worker Action:
Teach youth to share portfolios via secure PDF links instead of large attachments.

Outcome:
Youth demonstrate professional digital communication etiquette.

D. Worksheet: Digital Tool Inventory and Skills Gap Self-Assessment

This worksheet is designed to help you, the youth worker, assess your foundational digital skills and prioritize continuous professional development, ensuring you can meet the needs of diverse youth populations.

Part A: Digital Tool Inventory and Confidence

Tool Category	Tools I Use Regularly (List them)	My Confidence (1=Low, 5=High)	How I Use It for Youth Work (e.g., Tracking attendance, delivering a quiz)
Virtual Meetings (Zoom, Teams, Google Meet)			
Design/ Presentation (Canva, Google Slides, Genially)			
Data/Sheets (Excel, Google Sheets)			
Task Management Trello, Planner, Project Timeline			

Part B: Core Functional Skills Assessment

Functional Skill	My Current Ability (1=Not Confident, 5=Expert)	Training/ Resource Needed (What/Why)
Information Literacy: I can verify the legitimacy of a news source or online statistic in under 5 minutes.		
Communication: "I can run a 45+minute online session that keeps participants actively engaged through tools like polls, chat, and breakout rooms."		
Content Creation: I can convert a print resource into a mobile-friendly digital format quickly and effectively.		
Problem Solving: I can quickly fix common technical issues during an online session without disrupting the flow		
I can securely manage personal data so that only one trusted team member has access.		

03

Online Security and Privacy

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

Navigating the Digital World Safely and Responsibly

This module equips youth workers and educators with the essential knowledge and practical strategies needed to help young people (aged 16–25, including disadvantaged groups) protect their personal information, understand online risks, and build digital resilience in an increasingly complex digital environment.

The Needs Assessment Report (R1) revealed a significant lack of digital literacy related to security and privacy among youth in partner countries. Advanced cybersecurity skills remain underdeveloped, leaving young people vulnerable to threats such as cyberbullying, online harassment, misinformation, and social engineering. Module 2 directly supports EthiTech's core objective of increasing awareness and strengthening protective behaviors in the digital sphere.

A. Theoretical Explanation: Importance of Security and Privacy

A1. Distinguishing Online Security and Online Privacy

Youth workers must clearly understand and teach the difference between online privacy and online security, as both are essential for responsible digital citizenship.

Online Privacy (Data Control)

Online privacy refers to the protection of personal information and understanding how data is collected, stored, and used by third parties. It includes:

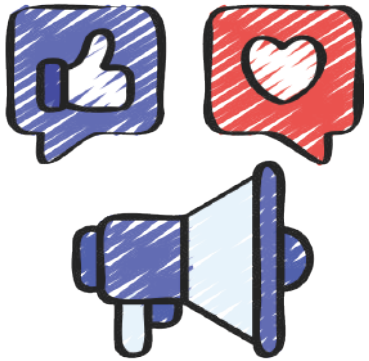
Managing privacy settings on social media

Controlling what information is shared publicly

Understanding data tracking and profiling

Configuring browser and app permissions

Privacy is fundamentally about who can access your information and how much control you have over it.



A2. Online Security (Safety and Resilience)

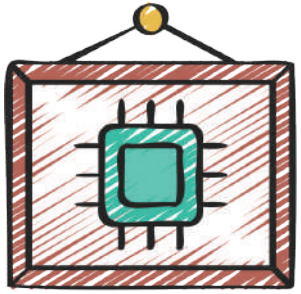
Online security refers to the behaviors, tools, and competencies needed to prevent or respond to harmful digital situations. It includes:

Strong passwords

Antivirus and firewall software

Safe browsing habits

Recognizing threats such as phishing or malware



Online security is a core component of Information Technology Security, a critical competency for the future workforce.

B. The Digital Risk Landscape and Social Engineering

The digital ecosystem exposes young people to a wide range of risks. One of the most dangerous is Social Engineering (SE)—the manipulation of human psychology to gain unauthorized access to sensitive information.

B1. Phishing Attacks

Phishing is the most common form of social engineering. Attackers use fake emails, websites, or messages to trick individuals into revealing:

Login credentials

Credit card numbers

Personal data

These attacks often appear legitimate, making them especially dangerous for inexperienced users.

B2. Attack Lifecycle: How Social Engineering Works

Social engineering attacks typically follow a predictable lifecycle:

Reconnaissance
The attacker gathers information about the target—interests, habits, social connections—often through social media or online research.

Planning
The attacker identifies vulnerabilities and chooses the most effective manipulation strategy.

Execution
The attacker launches the phishing email, fake website, or fraudulent message.

Exploitation
The attacker gains access to sensitive information or accounts.

B3. Proactive Security Measures

Youth workers should emphasize the following protective strategies:

Strong, unique passwords (minimum 12 characters)

Multi-Factor Authentication (MFA)

Using a VPN on public Wi-Fi

Understanding TLS encryption for secure communication

These measures significantly reduce the likelihood of successful cyberattacks.

Understanding this lifecycle helps youth recognize red flags before falling victim.

C. Global Data Protection and Legislative Frameworks (GDPR vs. CCPA)

Online privacy and security are reinforced by global legal frameworks such as:

GDPR — General Data Protection Regulation (EU)

CCPA — California Consumer Privacy Act (US)

Both laws guarantee strong protections for individuals regarding their personal data.

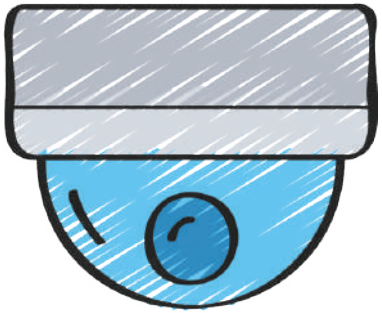
Understanding this lifecycle helps youth recognize red flags before falling victim.

C1. Shared Principles

- **Both GDPR and CCPA:**
- **Protect natural persons**
- **Define entities responsible for data processing (controllers/businesses)**
- **Define "processing/collecting" broadly**
- **Exclude anonymous or de-identified data**
- **Grant individuals the Right to Erasure/Deletion**

C2. Key Differences

Feature	GDPR (EU)	CCPA (California, US)
Entities Covered	Controllers (public, private, non-profit)	For-profit businesses meeting thresholds
Individuals Protected	Any identifiable person (no residency requirement)	California residents only
Special Data	Defines "special categories" (e.g., biometric data)	No separate category
Exclusions	Excludes purely personal/household processing	Excludes specific medical/clinical data
Focus	Legal grounds for processing	Transparency + opt-out of data selling
Children's Protection	Strong protections for minors	Parental consent for selling children's data



D. Practical Guidance: Key Strategies for Digital Resilience

Youth workers should focus on teaching concrete, actionable behaviors that strengthen digital resilience.

D1. Key Differences Account Security and Access Control

Strategy	Guidance for Youth Workers	Source References
Strong Password Management	Teach youth to use strong, unique passwords (12+ characters, mixed symbols). Avoid password reuse. Change passwords regularly.	----
Password Managers	Recommend password managers to store and autofill complex passwords securely.	----
Multi-Factor Authentication (MFA)	Encourage MFA on all critical accounts. MFA drastically reduces successful attacks.	----

D2. Device and Data Protection

Strategy	Guidance for Youth Workers	Source References
Software Updates	Keep operating systems and antivirus software updated.	----
Secure Connections (VPN)	Avoid personal transactions on public Wi-Fi. Use a VPN for encrypted communication.	----
Data Backup	Regularly back up important data to cloud or external drives.	----

D3. Privacy and Responsible Digital Behavior

Strategy	Guidance for Youth Workers	Source References
Managing Digital Footprints	Explain how online actions leave permanent traces. Encourage caution when sharing personal information.	----
Reviewing Privacy Settings	Teach youth to configure privacy settings on social media and browsers.	----
Closing Old Accounts	Encourage deleting unused accounts to reduce security risks.	----

D4. Avoiding Social Engineering and Phishing

Youth must learn to think critically before acting online.

Suspicious Links/Emails
Avoid clicking unknown links or attachments. Verify legitimacy directly with the source.

Meeting People Online
Apply the same caution as in real life—online identities may be fake.

Personal Information Disclosure
Never share passwords or sensitive data. Be cautious about what is posted publicly.

E. Real-Life Examples

Example 1: The Urgent "Account Deactivation" Email (Phishing)
Scenario:
A 19-year-old receives an email claiming their university account will be deactivated unless they "verify their identity" immediately.

Youth Worker Guidance:

Identify urgency as a manipulation tactic, Check sender address and link by hovering, Contact the university directly instead of clicking

Example 2: The Permanent Digital Footprint
Scenario:
A recruiter finds an old inappropriate post from a youth applying for internships.

Youth Worker Guidance:

Review digital footprint regularly, Clean up old accounts and posts, Reinforce ethical digital behavior

F. Practical Worksheet: The Digital Safety Audit

Step	Focus Area	Youth Task (Action Points)	Safety Tip/Reference
Access Control Check	Authentication & Passwords	Review your 3 most critical accounts (e.g., primary email, social media, bank). Verify if each uses a unique, strong password (min. 12 characters, mixed case, symbols).	Using the same password everywhere is a major weak spot. Use a Password Manager for complex passwords.
MFA Implementation	Multi-Factor Authentication	For those 3 critical accounts, verify that Multi-Factor Authentication (MFA) is enabled (e.g., text code, authenticator app, or biometrics).	MFA significantly decreases the likelihood of a successful cyberattack.
Privacy Settings Review	Data Control	Select your most used social media app. Navigate to its Privacy Settings section and check how public your information (photos, birth date, contact info) is. Adjust settings to the highest privacy level you are comfortable with.	Even if settings are private, little data online is totally private. Youth workers should provide guides on reviewing these settings.
Device Hygiene Check	System Security	Check your computer/phone settings: Is the Operating System updated to the latest version? Is Antivirus software installed and active?	Using the latest versions benefits from the latest security patches.
Phishing Recognition Drill	Threat Identification	Open your spam or junk folder (or review recent suspicious messages). Identify one message and write down the red flags (e.g., urgent tone, poor spelling, strange link address) that mark it as a potential scam.	Always think before acting; suspicious messages demand verification directly from the source.

04

Digital Creativity and Empowered Expression

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

Using Digital Tools for Expression, Innovation, and Youth Empowerment

This module explores the role of Digital Creativity in youth work, focusing on how young people—especially those from disadvantaged backgrounds—can use digital tools for self-expression, innovative problem-solving, and developing an entrepreneurial mindset. The goal is to help youth shift from passive digital consumers to active digital co-creators.

Digital Creativity as a Tool for Well-being and Inclusion

Emotional Outlet
Digital creative activities—such as digital art, music production, podcasting, or video editing—provide a safe, structured space for young people to express emotions, explore identity, and build confidence. These activities support mental well-being and help youth develop healthy coping mechanisms.

Democratization and Access
Digital tools have dramatically reduced barriers to creative expression. What once required expensive equipment can now be done with free or low-cost apps. This democratization is especially important for disadvantaged youth, enabling them to participate, express themselves, and feel represented—even when geographically isolated.

A Bridge for Digital Youth Work
Digital creativity is not a separate method—it is an integral part of modern youth work. It enhances engagement, supports diverse learning styles, and helps youth workers integrate digital tools into existing activities.

Theoretical Explanation: Creativity, Competence, and the Inclusion Imperative

Digital creativity is the ability to generate ideas or products that are both novel and valuable through the use of technology. Unlike basic functional digital skills, digital creativity emphasizes purposeful, transformative use of digital tools. It is a key driver of inclusion, empowerment, and youth engagement.

The Link to Employability and Entrepreneurship

Creativity is now recognized as a core soft skill essential for the future labor market, alongside critical thinking and collaboration.

Entrepreneurial Creativity
This concept focuses on using creative digital skills to build an entrepreneurial mindset. When youth design a marketing campaign, create a short film, or build a simple website, they learn:

How to communicate ideas

How to market their skills

How to navigate the creative economy

This directly supports EthiTech's goal of fostering initiative and employability.

Practical Guidance: Strategies for Fostering Digital Content Production

This section outlines practical strategies youth workers can use to help young people become active digital creators.

Strategy	Youth Worker Action (Detailed Steps)	Key Digital Tools & Focus
Leverage Existing Knowledge	Encourage youth to express opinions on local issues (e.g., mental health, pollution) using familiar formats like social media stories or short vlogs. Challenge them to create a "200-word video pitch" to focus on clarity and purpose rather than technical complexity.	Use YouTube, Instagram/TikTok formats, or simple video apps to reduce intimidation and increase participation.
Facilitate Collaborative Creativity	Organize group projects where youth co-create a digital artifact (e.g., a shared presentation, digital art piece). Teach teamwork, conflict resolution, and version control.	Use collaborative whiteboards (Miro), shared Google/Microsoft documents, or joint design platforms.
Encourage Meaningful Creation	Guide youth to connect their digital output to real-world causes or social issues. Digital Storytelling is especially powerful for marginalized youth to reclaim their narratives.	Use storytelling techniques to create short documentaries or advocacy campaigns.
Integrate Maker Activities & Gamification	Introduce coding workshops, robotics, or gamified learning quests. Use platforms like Actionbound to create location-based challenges requiring creative digital solutions.	Use coding bootcamps, robotics kits, or gamification tools to expand practical skills beyond screen-based creation.

Real-Life Example: Digital Storytelling for Social Inclusion

Digital Storytelling is one of the most impactful applications of digital creativity. It empowers marginalized youth to share their experiences, build confidence, and participate actively in society.

Target Group's Need	Youth Worker Action	Transformed Outcome & Project Alignment
Lack of Voice / Invisibility	Introduce basic video or podcast tools. Guide youth to create a short narrative about a personal challenge or community issue (e.g., accessing education as a migrant).	Self-Advocacy & Empowerment: Youth realize technology can be a tool for social contribution, not just entertainment.
Skill Gap & Employability	Teach storyboarding, scriptwriting, and editing basics to ensure a professional final product suitable for a portfolio.	Entrepreneurial Creativity: The final video/podcast becomes a portfolio asset demonstrating initiative and technical skill.
Civic Engagement	Encourage youth to share their story through organizational networks or social media, linking to Modules 1 and 2.	Active Citizenship: The story becomes an advocacy tool for community stakeholders or policymakers.

Worksheet: Digital Creativity Self-Assessment & Campaign Planning

This worksheet is designed specifically for youth workers and trainers (T2 target group) to accomplish two goals: 1) Audit their own capacity to deliver the content, and 2) Pre-plan an inclusive, creative activity that aligns with the project's objectives (employability and social advocacy).

Part A: Digital Creativity Tool Confidence (Capacity Building)

This section helps youth workers assess their own ability to use digital creativity tools effectively. The goal is to ensure that trainers have the technical fluency required to guide young people through creative digital activities. If a trainer rates themselves at a low level (1 or 2), this indicates an immediate need for professional development before delivering the training.

The first component assessed is digital design fluency. Being able to use tools such as Canva or Adobe Spark is essential for supporting young people in producing professional-looking outputs, including digital CVs, portfolio flyers, or visual storytelling materials. These outputs are directly linked to employability, and trainers must feel confident teaching these tools to help young people build strong digital portfolios.

The second component focuses on gamification and digital quest design. Platforms like Actionbound allow trainers to transform learning into an interactive, engaging experience. This skill is especially valuable for young people who struggle with traditional learning methods, as gamification increases motivation, participation, and knowledge retention. Trainers who can design gamified activities create more dynamic and inclusive learning environments.

The third component evaluates the trainer's ability to use digital collaboration platforms, such as Miro or virtual whiteboards. These tools enable structured co-creation, brainstorming, and group problem-solving. Mastery of these platforms ensures that trainers can facilitate safe, organized, and collaborative creative processes. This competency is essential for preparing young people for the digital workplace, where teamwork and shared digital production are core expectations.

Part B: The Purposeful Content Plan (Project Alignment)

This section ensures that youth workers not only understand digital creativity tools but also design creative activities that align with the EthiTech project's goals of inclusion, active citizenship, and entrepreneurship. The focus is on making sure that every creative output produced by young people is meaningful, relevant, and socially impactful.

The first step is identifying the young person's interests and passions. Effective youth work must be grounded in the lived experiences and motivations of the participants. When creative projects reflect what young people genuinely care about, engagement increases and the final output becomes more authentic and powerful.

The second step involves defining a clear creative goal and a tangible output. Whether the final product is a two-minute short film, a podcast episode, a digital poster, or a simple website prototype, having a concrete outcome helps structure the creative process. It also ensures that the final product can be added to the young person's professional portfolio, linking creativity directly to employability and future opportunities.

The third and most critical step is establishing an inclusion mandate and voice strategy. The trainer must intentionally consider how the creative project will give visibility and voice to young people who often feel unheard—such as refugees, migrants, rural youth, or those facing economic hardship. This transforms digital creativity from a technical exercise into a tool for social advocacy and empowerment. Through storytelling and creative expression, young people can highlight their experiences, challenge stereotypes, and contribute to community dialogue.

05
Digital Citizenship

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

Ethical, Responsible, and Empowered Participation in the Digital Society

This module moves beyond basic "internet safety" and introduces a comprehensive framework for understanding and practicing digital citizenship. It equips youth workers, educators, and learners with both theoretical foundations and practical tools to become ethical, responsible, and active participants in the digital world.

I. Theoretical Explanation: Defining Digital Citizenship in the 21st Century

Digital Citizenship refers to the norms of appropriate, responsible, and empowered technology use. It is not a simple list of rules like "don't bully" or "don't hack"—it is a proactive mindset that encourages individuals to use technology to contribute positively to their communities and build a meaningful digital identity.

The Concept of the Digital Self

Modern psychology recognizes that our online and offline selves are deeply interconnected. The Online Disinhibition Effect shows that people may behave differently online due to perceived anonymity and lack of real-time feedback. Digital citizenship education aims to bridge this gap, helping young people align their digital actions with core values such as empathy, integrity, and accountability.

The 9 Elements of Digital Citizenship (Ribble's Framework)

To make the broad and complex concept of digital citizenship easier to understand and teach, Ribble organizes it into nine elements, grouped under three guiding principles: Respect, Educate, and Protect. Together, these elements form a holistic model for ethical, informed, and safe participation in the digital world.

A. Respect — Social & Ethical Standards

Digital Etiquette

Often referred to as "netiquette," digital etiquette goes far beyond basic politeness. It involves understanding the unwritten rules and cultural norms of different digital platforms. What is acceptable on a Discord server—such as slang, memes, or informal language—may be inappropriate or even harmful on LinkedIn or in a professional email. Effective digital citizens understand tone, timing, and context across platforms.

Digital Law

Digital law refers to understanding the legal rights and restrictions that govern technology use. This includes: Copyright & Fair Use: Recognizing that images found on Google cannot be freely used in commercial or public presentations. Cybercrime Awareness: Understanding that hacking, identity theft, malware creation, and hate speech are criminal offenses—not harmless pranks.

Digital Access

Digital access focuses on ensuring equitable opportunities to participate in the digital world. A responsible digital citizen advocates for closing the Digital Divide, recognizing that not everyone has access to high-speed internet, modern devices, or digital learning opportunities. Limited access creates significant social and economic inequalities.

B. Educate — Cognitive & Intellectual Growth

Digital Literacy

Digital literacy is the ability to use digital tools effectively and evaluate the information encountered online. It is the primary defense against misinformation and "fake news." Digitally literate individuals can cross-reference sources, identify bias, and understand how algorithms shape their online experience—creating echo chambers that reinforce certain viewpoints.

Digital Communication

Digital communication involves understanding the wide range of communication modes—email, instant messaging, video calls, social media posts—and choosing the appropriate channel for the message. For example, ending a relationship via text or resigning from a job through a tweet reflects poor digital judgment. Effective digital citizens match the message to the medium.

Digital Commerce

Digital commerce refers to the safe and intelligent buying and selling of goods online. This includes: Understanding consumer protection rights Recognizing subscription traps Verifying secure websites (HTTPS) Being aware that personal data often functions as "currency" in free apps and platforms

C. Protect — Safety & Security

Digital Commerce

Digital health and wellness address both physical and psychological well-being in digital environments. Physical Health: Ergonomics, preventing eye strain, avoiding text neck, and maintaining healthy device posture. Psychological Health: Managing screen time, recognizing signs of internet addiction, and understanding the mental health impacts of social comparison and FOMO.

Digital Literacy

Just like in the physical world, digital citizens have rights—such as privacy and freedom of expression—and responsibilities, such as reporting cyberbullying, respecting others' data, and avoiding harmful behavior. Digital citizenship requires balancing personal freedoms with respect for others.

Digital Communication

This element focuses on the technical measures individuals must take to protect their identity, data, and devices. Key practices include: Using password managers Enabling Two-Factor Authentication (2FA) Following the 3-2-1 Backup Rule (3 copies of data, 2 different storage types, 1 off-site backup)

The S3 Framework

To simplify the nine elements of digital citizenship for everyday use, EthiTech applies the S3 Framework, which organizes digital behaviors into three practical categories:

Safe: Protecting yourself and others through security, privacy, and healthy digital habits.

Savvy: Making informed, educated choices by understanding digital literacy, online commerce, and digital law.

Social: Respecting yourself and others by practicing etiquette, promoting access, and upholding digital rights.

II. Practical Guidance

The "THINK" Method for Content Posting

The fast and impulsive nature of digital communication often leads people to post without reflection. The THINK method helps young people and educators pause before interacting online, reducing the risk of misinformation, conflict, or regret.

T – Is it True?
Before sharing, verify the accuracy of the information. Is the source reliable? Could you be spreading a rumor?

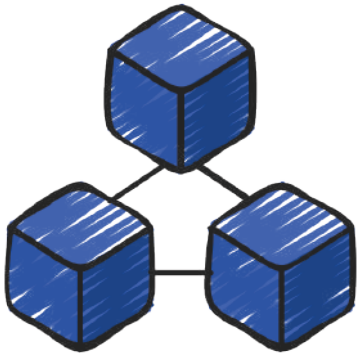
H – Is it Helpful?
Does your post add value, support, or constructive insight? Or is it simply negativity or unnecessary noise?

I – Is it Inspiring?
Does the content reflect the best version of your digital self? Does it uplift or motivate others?

N – Is it Necessary?
Is this something that truly needs to be shared publicly? Would this conversation be more appropriate in private? Are you oversharing personal information?

K – Is it Kind?
Apply the "Grandmother Rule": Would you feel comfortable if your grandmother read this post?

The THINK method encourages mindful, respectful, and responsible digital behavior.



Professional Netiquette Guidelines

Professional digital communication plays a crucial role in building trust and credibility in both educational and workplace settings. The following guidelines help young people develop strong digital professionalism:

The Subject Line Rule
Never send a professional email without a clear and descriptive subject line. It sets expectations and improves communication efficiency.

Reply-All Discipline
Use "Reply All" only when every person in the thread genuinely needs to see your response. Overuse creates confusion and unnecessary notifications.

Tone Awareness
Written communication lacks nonverbal cues, making tone easy to misinterpret. Avoid sarcasm unless you know the recipient very well. Emojis can clarify intent in informal contexts, but they should not appear in formal reports or professional documents.

Respecting Others' Privacy
Never forward a private email or share a screenshot of a private chat without explicit permission from the sender. Doing so violates trust and ethical communication norms.

These guidelines help young people navigate digital spaces with professionalism and respect.

Managing Your Digital Footprint

This includes all content intentionally created by the user: social media posts, comments, uploaded photos, and public interactions. Managing it requires thoughtful posting and awareness of long-term consequences.

Passive Digital Footprint

This consists of data collected automatically without the user's direct input: IP addresses, browsing history, cookies, and location data.
It can be managed by:

Using privacy-focused browsers

Connecting through a VPN

Regularly clearing cookies and browsing history

Effective digital footprint management helps young people maintain a positive online identity and safeguard their personal information.

III. Real-Life Examples (Case Studies)

Real-life scenarios help young people understand how digital citizenship principles apply in everyday situations. The following case studies illustrate common ethical, legal, and safety challenges in the digital world and highlight why responsible online behavior is essential.

Case Study 1: The "Harmless" Meme (Digital Law & Ethics)

In this scenario, Sarah, a marketing intern, prepares a presentation for her company's new product launch. Wanting to make the presentation more entertaining, she adds a popular meme character and uses a hit pop song as background music. The presentation is later uploaded to the company's public YouTube channel.

Shortly after, the video is flagged for copyright infringement due to the unauthorized use of the song. Additionally, the original creator of the meme artwork threatens legal action because their image was used for commercial purposes without permission.

This case demonstrates that "Fair Use" is extremely limited, especially in commercial contexts. Digital Citizenship—specifically Digital Law—requires verifying the licensing of all digital assets before using them. Sarah should have selected royalty-free music and licensed or Creative Commons images to avoid legal and ethical violations.

Case Study 2: The Screenshot Betrayal (Privacy & Etiquette)

In a private Discord conversation, Liam confides in his friend Mark about his frustrations with their boss. It is a moment of vulnerability shared in confidence. Mark, thinking it will be amusing, takes a screenshot of the message and posts it in the general office WhatsApp group.

As a result, Liam faces disciplinary consequences, but the deeper issue is the breakdown of trust within the workplace. Mark defends himself by saying, "I didn't say it—Liam did!" However, the real harm comes from Mark's decision to expose a private conversation.

This case highlights a serious violation of Digital Rights (Privacy) and Digital Etiquette. Even though Liam wrote the message, Mark is more at fault for weaponizing private communication. It also reinforces a key principle of digital citizenship: digital communication is permanent—anything shared online can be captured, forwarded, or misused. Young people must learn to treat private messages with the same confidentiality as in-person conversations.

Case Study 3: The "Deepfake" Dilemma (Literacy & Ethics)

A high school student uses an AI tool to swap a classmate's face onto a video of someone doing something embarrassing. Believing it to be a harmless joke, they share the edited video with others.

The video spreads rapidly, and even though it is artificial, the emotional harm and humiliation experienced by the victim are very real.

This case touches on both Digital Safety (cyberbullying) and Digital Literacy (understanding AI technologies). Creating non-consensual synthetic media is a serious ethical violation and is illegal in many regions. Young people must understand the power and risks of AI tools and the importance of consent, dignity, and empathy in digital spaces.

III. Real-Life Examples (Case Studies)

Worksheet A: The S3 Digital Health Check

This self-assessment tool helps individuals evaluate their digital citizenship habits across the three pillars of the S3 Framework: Safe, Savvy, and Social. Participants rate themselves on a scale from 1 (Needs Work) to 5 (Expert) for each statement. The goal is to promote self-awareness and identify areas for improvement in digital behavior, security, and responsibility.

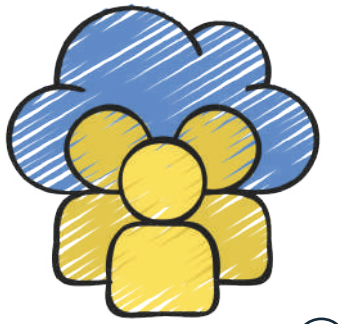
After completing the assessment, participants calculate their total score:

0–15: Digital Rookie — A foundational understanding is needed; reviewing the Nine Elements of Digital Citizenship is recommended.

16–35: Digital Citizen — Good habits are in place, with room for continued improvement.

36–45: Digital Leader — Strong digital citizenship skills; individuals in this range are well-positioned to mentor and support others.

This worksheet encourages honest reflection and helps youth workers identify which areas require additional training or support.



Worksheet B: The "Feelings & Options" Dilemma Solver

Use this whenever you face a difficult online situation (e.g., witnessing bullying, receiving a suspicious message).

Step	Question	Your Answer
1. Identify	Who is involved? (Victim, aggressor, bystanders, authorities)	
2. Feel	How does the victim feel? How does the aggressor feel?	
3. Imagine	Option A: Ignore it. (Consequence: _____)	
	Option B: Report privately. (Consequence: _____)	
	Option C: Confront publicly. (Consequence: _____)	
4. Decide	Which option creates the most positive outcome for the community?	
5. Act	Draft the message or list the specific steps you will take now.	

06

Social Media Management

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

Building a Positive Digital Identity and Healthy Habits

This module equips youth workers and educators with the knowledge and tools to help young people (aged 16–25, including those from disadvantaged backgrounds) transition from passive social media consumers to active, intentional managers of their digital presence. It focuses on understanding algorithms, shaping a positive digital identity, and maintaining mental well-being in a hyper-connected world.

I. Theoretical Explanation: The Mechanics of Engagement

The Algorithm: The Invisible Editor

Social media feeds are not neutral or chronological. They are curated environments shaped by algorithms designed to maximize user engagement.

The Attention Economy

Social media platforms operate on an attention-based business model. Their primary goal is to keep users online as long as possible to display more advertisements. Algorithms predict which content will generate the most engagement—likes, comments, shares, watch time—and prioritize it above all else.

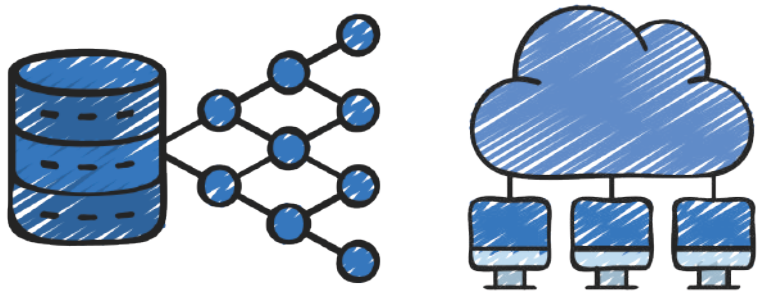
The Feedback Loop

Every user action becomes a data point:

Watching a video to the end

Liking a photo

Hovering over a post



The algorithm interprets these behaviors as “interest” and shows more similar content. If a young person interacts with negative or sensational posts, the algorithm amplifies that content, creating a self-reinforcing cycle.

Filter Bubbles and Echo Chambers

Filter Bubbles:
Algorithms prioritize content that aligns with the user's existing beliefs to keep them comfortable and engaged.

Consequence:
Young people may begin to believe that "everyone" shares their viewpoint, reducing exposure to diverse perspectives and increasing polarization.

Digital Identity: Active vs. Passive Footprints
A digital identity is the sum of all data a person leaves behind online—both intentionally and unintentionally.

Active Digital Footprints
These include posts, comments, photos, videos, and any content a user deliberately shares. This forms the "public brand" a young person presents to the world.

Passive Digital Footprints
These are collected automatically, often without awareness:

IP addresses, Browsing history ,Device information, Location data

Even silent browsing ("lurking") contributes to a passive footprint that shapes the ads and content a user sees.

Context and Permanence
Context Collapse:
A joke intended for friends can be taken out of context by a future employer or university.

The Long Tail of Data:
Digital content is searchable, replicable, and long-lasting. A careless comment made at 16 can resurface years later during a background check.

The Psychology of Engagement: Why We Scroll
Social media platforms leverage psychological triggers to keep users engaged.

The Dopamine Loop
Likes, comments, and notifications trigger dopamine release, creating a reward cycle similar to gambling. The unpredictability of rewards keeps users checking apps compulsively.

Social Comparison and Self-Esteem
Users compare their everyday lives to others' "highlight reels." This can lead to:

Anxiety, Low self-esteem,
Depression

This "compare and despair" effect is especially strong among adolescents.

FOMO (Fear of Missing Out)
Constant updates create anxiety about missing experiences. This leads to:

Late-night scrolling, Sleep disruption,

Reduced focus, Increased irritability

Understanding these psychological mechanisms helps young people regain control over their digital habits.

II. Practical Guidance: Strategies for Youth Workers

"Retraining" the Algorithm
Youth workers can teach young people that they have control over their feed.

Action:
If a feed is filled with negative or unhelpful content, users can retrain the algorithm by intentionally engaging with positive, educational, or hobby-related posts.

Guidance:
Stop hate-watching. If you interact with drama, the algorithm gives you more drama. Interact with growth, and it gives you growth.

The "Grandma Test" for Content Creation
Before posting, young people should ask:
"Would I be comfortable if my grandmother, a future employer, or a teacher saw this?"
If the answer is no, they should not post.

Privacy Reminder:
Private accounts are not truly private—screenshots can be shared anywhere.

Intentional vs. Mindless Scrolling
Encourage youth to shift from passive "doomscrolling" to intentional use.

Time Management
Use built-in digital wellbeing tools to set daily limits for apps.

Purposeful Use
Log in with a clear intention:
"I'm opening this app for 15 minutes to message friends and check my hobby group."

This reduces compulsive checking and improves mental well-being.

III. Real-Life Examples

Example 1: The "Viral" Mistake (Reputation Management)
Scenario:
A 17-year-old posts an angry rant about their manager on Instagram Stories, assuming it will disappear in 24 hours. A co-worker screenshots it and shares it with the manager. The student is fired and struggles to get a reference.

Lesson:
Nothing online is temporary. Digital reputation affects real-world opportunities.

Better Approach:
Vent offline or in a private, encrypted chat—not on public platforms.

Example 2: Breaking the Echo Chamber (Algorithm Literacy)
Scenario:
A young person notices their TikTok feed only shows political content that confirms their existing beliefs. They begin to assume "everyone" thinks the same way.

Lesson:
The algorithm is creating a filter bubble.

Better Approach:
Actively search for reputable sources with diverse perspectives and engage with varied content to rebalance the feed.

IV. Practical Worksheet: The Social Media Audit

Step	Focus Area	Youth Task (Action Points)	Safety Tip / Reference
1. The Reputation Scan	Digital Footprint	Search your name and username in Incognito Mode. Review the first 5 images/links.	If negative content appears, delete it or request removal from the site admin.
2. Feed Detox	Mental Health	Review your "Following" list. Unfollow at least 5 accounts that make you feel insecure, angry, or unhappy.	Curating your feed protects mental health from negative comparison.
3. Privacy Lockdown	Security	Check tagging settings. Require approval before tagged photos appear on your profile.	Prevents others from shaping your digital identity without consent.
4. Algorithm Retrain	Content Control	Visit your Explore page. Like/save 3 posts related to a skill you want to learn.	Signals the algorithm to prioritize educational content.
5. Time Check	Well-being	Review last week's screen time. Identify the most time-consuming app and set a daily limit.	Reducing passive scrolling improves sleep and focus.

07

Digital Storytelling

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

Amplifying Voices and Crafting Identity

This module equips youth workers to support young people—especially migrants, refugees, and those from disadvantaged backgrounds—in using digital tools to craft and share their personal narratives. Digital Storytelling (DST) goes far beyond simple video creation; it is a structured methodology that centers identity, agency, and ethical responsibility in the digital public sphere.

A. Theoretical Explanation: The Art and Ethics of Digital Narratives

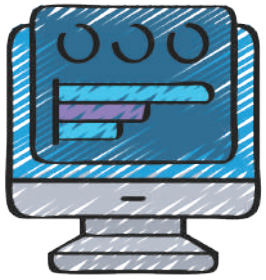
Digital Storytelling combines personal narrative with digital media—images, voice, music—to create short, meaningful stories. Understanding the theory behind DST helps youth workers facilitate the process with sensitivity and purpose.

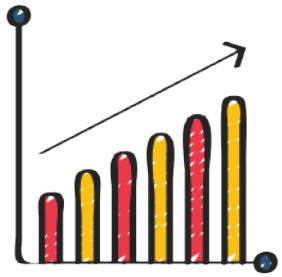
A.1 Identity Formation and the "Democratization of Voice"
For young people, especially those who have experienced displacement or marginalization, telling their story is a powerful act of identity construction.

Reclaiming the Narrative
Marginalized groups are often spoken about rather than given the opportunity to speak for themselves. DST reverses this dynamic by enabling youth to become creators rather than subjects of representation.

Therapeutic Potential
While youth workers are not therapists, the process of shaping chaotic life experiences into a coherent narrative can help young people make sense of trauma, build resilience, and strengthen their sense of belonging.

The "Crowded Talk" Concept
Youth voice develops socially, not in isolation. DST workshops create a reciprocal learning environment where participants learn from each other's lived realities, fostering empathy and collective understanding.





A.2 The Seven Elements of Digital Storytelling
Joe Lambert's framework distinguishes a true digital story from a simple slideshow or music video. Youth workers should guide participants through these seven core elements:

Point of View: Stories must be personal and subjective. "I" statements are essential.

The Dramatic Question: A compelling hook that keeps the viewer engaged until the end.

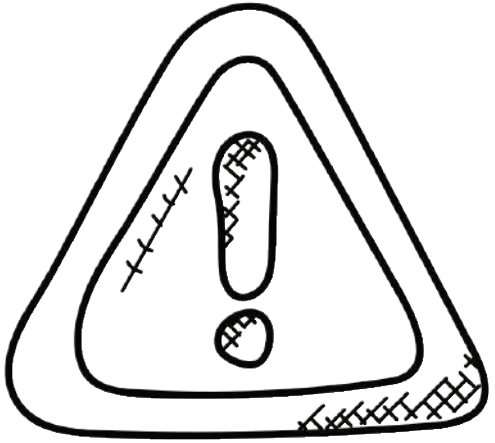
Emotional Content: Stories should evoke emotion—joy, sadness, empathy, reflection.

The Gift of Your Voice: A personal voiceover adds authenticity and individuality.

The Power of the Soundtrack: Music should support, not overpower, the narrative.

Economy: Short, focused stories (2–3 minutes) are more impactful.

Pacing: Rhythm and timing shape the viewer's emotional journey.



A.3 Narrative Architecture for the "TikTok Generation"
Short-form platforms require adapted storytelling structures.
The classic three-act structure can be condensed into 30 seconds:

Act 1 (0–3s): The Hook — a striking visual or bold statement

Act 2 (4–25s): The Value or Conflict — the core message

Act 3 (26–30s): The Payoff — resolution or call to action

This structure helps youth communicate meaningfully within fast-paced digital environments.

A.4 Visual Literacy
Images are not neutral. Youth must learn to "read" and "write" visual meaning.

Visual Metaphor
Using symbolic imagery—such as a storm cloud to represent sadness—helps youth express complex emotions and enhances higher-order visual literacy.

A.5 The Ethics of "Do No Harm"
Ethics are essential when working with vulnerable youth.

Informed Consent
Consent must be fully understood—not just signed. Youth should know where their story will be shared and that they can withdraw at any time.

Anonymity vs. Recognition
Some youth want visibility; others need protection. Options include: Blurring faces, Using illustrations

B. Practical Guidance: From Concept to Screen

B.1 The Story Circle (Pre-Production)
Before using any technology, gather participants in a circle.

Prompts: "Tell a story about a challenge you faced" or "Describe a moment that changed you."

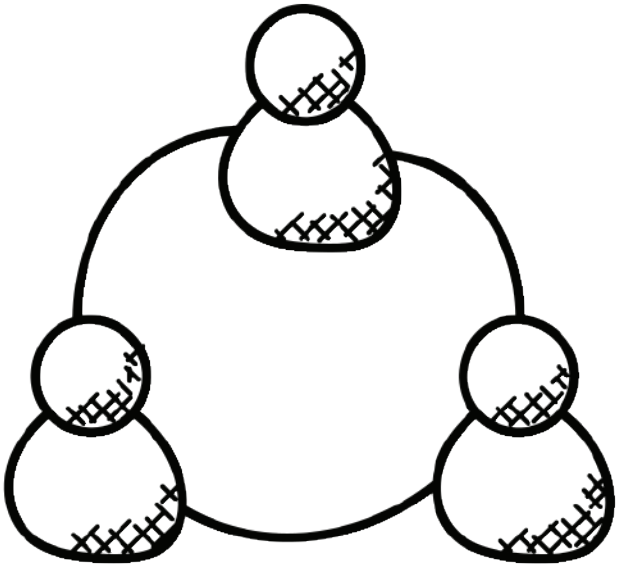
Feedback: Focus on the story, not the technical aspects. This builds trust and peer support.

B.2 Economy and Scripting
Word Count Rule: ~2 words per second. A 1-minute story ≈ 120 words.

Write for the Ear: Encourage conversational, natural language rather than academic writing.

2.3 Visual Storyboarding
Use the Think Aloud method:
"What do you see?"
"What makes you say that?"

Then create a storyboard with three columns: **Script / Visual / Audio.**
This prevents confusion during editing.



2.4 The Edit (Production)
Use accessible tools (smartphones, Canva, CapCut) to ensure equity.

Editing order:

Voiceover (foundation)

Visuals (match the words)

Music (support the mood)

C. Real-Life Examples

Example 1: The "Anonymous" Journey (Ethics in Action)
Scenario: A young refugee wants to tell the story of their journey, but fears for their family back home.
Application: The youth worker helps them use visual metaphors (feet walking on different roads, shots of hands packing a bag, sketches of the border) instead of filming their face. They record the voiceover but use audio software to slightly lower the pitch.
Result: The story is powerful and authentic ("The Gift of Voice") but protects the creator's identity ("Do No Harm").

Example 2: The 30-Second Advocate (Short-Form Structure)
A youth group wants to raise awareness about local pollution.
Application: Hook: Fast cuts of trash with text "This is our backyard."
Confrontation: Voiceover explaining environmental impact
Resolution: "Join us Saturday at 10 AM" (Call to Action)
Result: High engagement and clear messaging suitable for TikTok/Instagram.

D. Practical Worksheet: The Digital Story Canvas

Section	Question / Prompt	Action for Youth	Theory Reference
1. The Core Message	What is the ONE emotion you want the audience to feel?	Write one emotion (e.g., hope, anger, nostalgia).	Emotional Content
2. The Dramatic Question	What question keeps the viewer watching?	Write a guiding question.	Dramatic Question
3. The Hook (Visual)	What is the first image the audience sees?	Sketch or describe a striking visual.	Pacing / Visual Hooks
4. The Voice	Who is telling the story?	Write the first sentence starting with "I...".	Point of View
5. The Safety Check	Does this story put anyone at risk?	Tick safety boxes (no faces without consent, no revealing locations).	Ethics / Do No Harm
6. The Audio Layer	What music or sound supports the emotion?	Describe the sound (e.g., soft piano, silence).	Soundtrack

08

Detecting Fake News & Media Literacy

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

Navigating the Information Disorder

This module equips youth workers to help young people—especially migrants, refugees, and those from disadvantaged backgrounds—distinguish truth from manipulation in today's chaotic digital landscape. It goes beyond simple fact-checking and explores why misinformation spreads, how it targets vulnerable communities, and how young people can build the skills to resist harmful narratives.

The goal is to transform youth from passive consumers into active, critical "digital detectives."

I. Theoretical Explanation: Understanding Information Disorder

The term "fake news" is catchy but misleading. It oversimplifies a complex ecosystem of falsehoods, manipulations, and harmful narratives. This module uses the Information Disorder Framework developed by the Council of Europe, which breaks the problem into clear categories and analytical components.

The Spectrum of Information Disorder
Information disorder exists on a spectrum defined by two factors: truthfulness and intent to harm.

Misinformation
False + No Harm Intent
Shared by people who believe it is true.

Example: Sharing an old storm photo thinking it is happening today.

Even without malicious intent, misinformation can still cause harm.

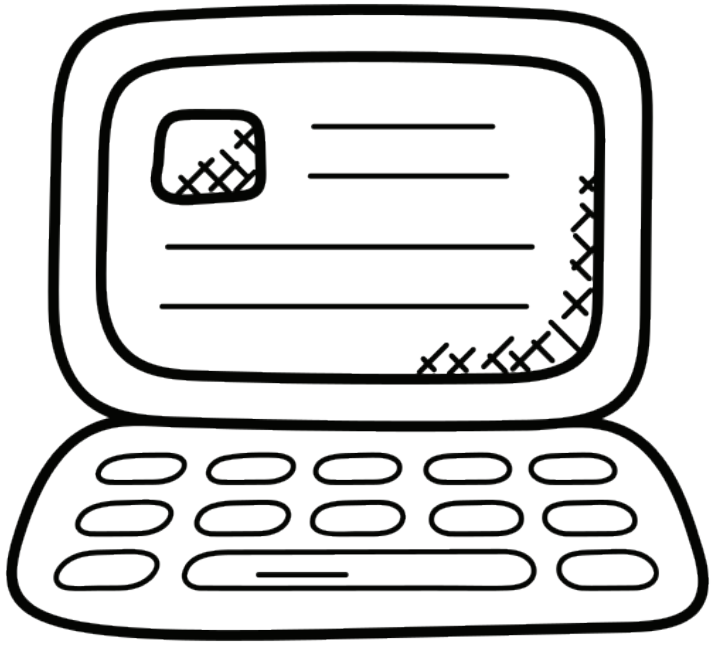
Disinformation
False + Harm Intent
Created deliberately to deceive or damage.

Examples:

Fabricated stories to suppress voter turnout

Conspiracies designed to incite hatred against refugees

Disinformation is often systematic, coordinated, and financially or politically motivated.



Malinformation
True + Harm Intent, Real information shared to cause harm. Examples: Doxing (leaking private information), Publishing someone's medical records to ruin their reputation, The facts are real, but the context is weaponized.

The Three Elements: Agent, Message, Interpreter
Youth must learn to analyze not just the content, but the entire ecosystem around it.

The Agent (Who?)
Who created the content?

Passionate individuals

State-sponsored troll farms

Financial opportunists seeking ad revenue

Understanding motivation (political, financial, ideological) is key.

The Message (What?)
What form does the content take?

Emotional memes

Manipulated videos

Imposter news articles mimicking real outlets

Visual formats often bypass critical thinking more easily than text.

The Interpreter (You)
The user's worldview shapes how they interpret content.

The same meme can be seen as satire by one person and "proof" by another.

This highlights the importance of self-awareness and bias recognition.

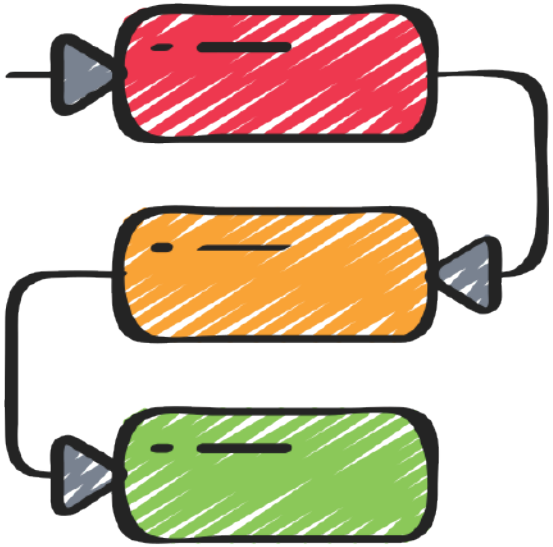
The Psychology of Belief: Why Our Brains Fail Us
Disinformation exploits human psychology.

Confirmation Bias & Motivated Reasoning
We seek information that confirms our beliefs and reject what challenges them.

The Continued Influence Effect
Even after a lie is corrected, it leaves a "memory trace" that continues to influence thinking.

This is why pre-bunking (warning people before they encounter a lie) is more effective than debunking.

The Backfire Effect
Sometimes correcting misinformation strengthens the false belief—especially when identity is threatened. However, clear and respectful corrections reduce this risk.



The Economics of Attention
Disinformation spreads because it is profitable. In the Attention Economy, human attention is a scarce commodity that platforms sell to advertisers.

Algorithmic Amplification: Social media algorithms are designed to maximize engagement (time on app). Content that triggers "Hot States" (high-arousal emotions like anger, fear, or outrage) generates the most engagement.

The Profit Loop: Therefore, algorithms naturally promote polarizing disinformation over boring, nuanced truths. Youth must understand that "if it makes you angry, it's probably making someone else money".

Visual Manipulation: Deepfakes vs. Shallowfakes
Visual evidence is trusted more than text, making it a prime vehicle for manipulation.

Shallowfakes (Cheap Fakes): These require low technical skill. They involve simply miscontextualizing a real photo (e.g., claiming a photo of a protest from 2015 is happening "right now") or slowing down a video to make a speaker sound drunk. This is currently the most common form of visual disinformation.

Deepfakes (Synthetic Media): These use AI and deep learning to swap faces or clone voices. While harder to make, they are becoming accessible.

Example: Creating a video of a politician declaring war or a celebrity endorsing a scam. The danger is not just that people believe the fake, but the "Liar's Dividend"—where people start doubting real evidence because "it could be a deepfake".

Scapegoating and "Othering"
For the specific target group of this project (migrants/refugees), misinformation often follows the pattern of Othering.

Narrative Framing: Disinformation campaigns frame migrants as threats to health, safety, or economic stability to mobilize local populations.

Dehumanization: By using language like "swarm" or "invasion," these narratives strip migrants of human dignity, making it psychologically easier for the public to accept harmful policies or violence against them.

II. Practical Guidance: Building Digital Detectives

For youth workers, the goal is to move young people from being passive consumers of information to active "digital detectives." This requires breaking old habits (like judging a website by how professional it looks) and building new reflexes. The core strategy we advocate is Lateral Reading combined with the SIFT Method.

The Core Technique: Lateral Reading
Most people read "vertically"—they stay on the webpage, scroll down, read the "About Us" page, and look for professional logos to decide if it is trustworthy. This is a mistake. Bad-faith actors know how to make professional-looking websites and fake "About Us" sections. Lateral Reading means leaving the site immediately to see what the rest of the web says about it.

The Tab Rule: Teach youth that as soon as they land on an unfamiliar source, they should open a new browser tab.

The Search Query: Instead of reading the article, search for the name of the site plus keywords like "funding," "bias," "controversy," or "reliable" (e.g., "The Daily News reliability").

Wikipedia Check: Look for the Wikipedia page of the media outlet. Wikipedia has strict community standards for sources. Check the "warning banners" at the top of the page or the "Political alignment" section in the sidebar. If a site is known for state propaganda or conspiracy theories, Wikipedia usually flags it immediately.

The SIFT Method (Advanced Breakdown)
Developed by Mike Caulfield, SIFT is a series of four "moves" to make when confronting a claim. Youth workers should teach these not just as steps, but as a habit loop.

FIND Better Coverage
Look for the same story in three reputable outlets. If no major outlet covers it, it's likely false.

Click through scientific links—often the study says the opposite of the claim.

Stop (The Emotional Circuit Breaker)
The Trigger: Misinformation is designed to hijack the brain's emotional center (the amygdala). If a post makes a young person feel shock, intense anger, fear, or validation ("I knew it!"), that is a red flag.

The 30-Second Rule: If you feel an emotional spike, put the phone down for 30 seconds. Do not share, do not comment, do not engage. Engaging with the content signals the algorithm to show it to more people.

The Purpose: The pause allows the "rational brain" (prefrontal cortex) to catch up with the emotional reaction.

Investigate the Source
Platform vs. Publisher: Teach youth to distinguish between where they saw it (e.g., "I saw it on TikTok") and who created it (e.g., "@FreedomPatriot123"). TikTok is the platform; the user is the publisher.

Hover and Click: Hover over the user's handle. Is the account brand new? Does the bio contain extreme language? A "blue check" does not always mean a source is an expert; on some platforms, it just means they paid for a subscription.

The Expertise Check: Ask: "Is this person in a position to know?" A doctor is an expert on medicine, but a doctor of philosophy is not an expert on vaccines. Misinformation often uses "experts" from irrelevant fields to borrow credibility.

Trace Claims to Original Context
Check if the image or quote is old, cropped, or misrepresented. Reverse image search is essential.

Visual Forensics: Analyzing Images and Video
Since visuals are powerful vectors for disinformation, youth need specific observation skills:

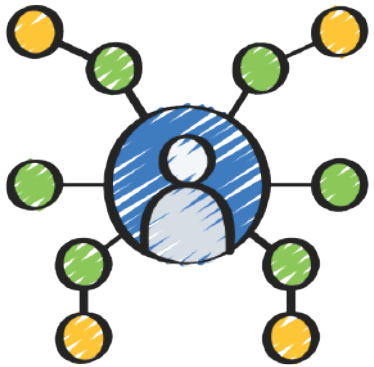
Reverse Image Search: This is the most powerful tool. Teach youth to use Google Lens, TinEye, or the Yandex image search (which is often better for facial recognition).
How-to: Upload the screenshot. If the image appears in articles from 2018, 2015, and 2012, it is obviously not "breaking news" from today.

The "Shadow and Sign" Check: Look at the background details. Weather: Does the post claim the protest was yesterday in Berlin? Check the weather history. If it was raining in Berlin but the sun is shining in the video, it's fake. Language: Look at street signs, shop names, or license plates. If the post claims to be from France but the stop signs say "ALTO" (Spanish) or the cars drive on the left, the location is a lie.

Pre-bunking: The "Inoculation" Strategy
Prepare youth before they encounter misinformation.

Tools:
"Bad News" game, "Go Viral" game
These teach manipulation tactics by letting youth play the role of a troll.

Pattern recognition:
"If a post blames all problems on one vulnerable group, it's using scapegoating."



III. Real-Life Examples

Example 1: The "Secret Benefits" Myth
A WhatsApp graphic claims migrants receive €2,000/month in cash benefits.

Analysis: Disinformation targeting intergroup conflict.

SIFT Application:

Investigate: Anonymous account with hate speech history

Find: Official government data disproves the claim

Result: Youth recognize the manipulation.

Example 2: The Deepfake Celebrity Endorsement
A footballer appears to promote a crypto scam.

Analysis: Synthetic media.

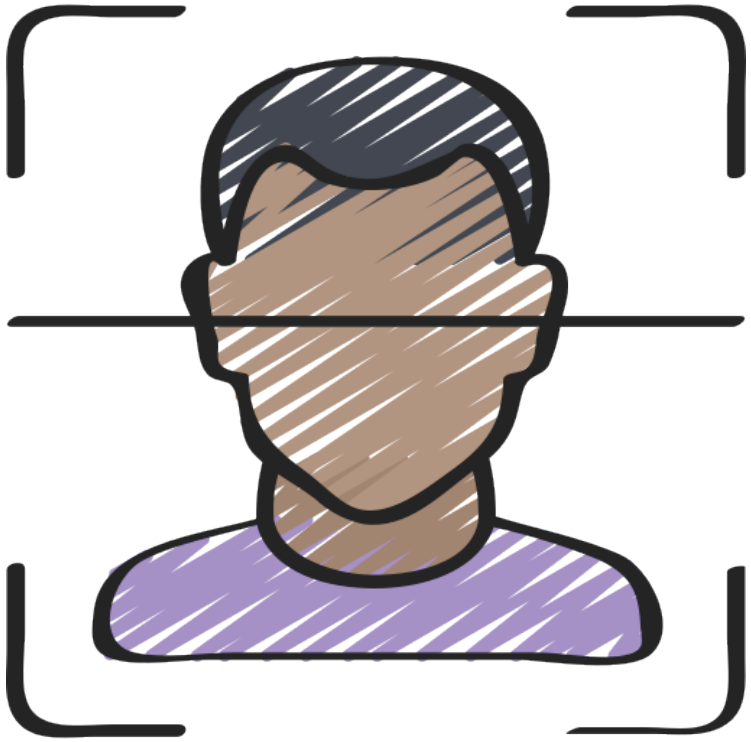
SIFT Application:

Trace: Reverse image search reveals original interview

Audio is AI-generated

Result: Youth report the scam instead of falling for it.

IV. Practical Worksheet: The Fact-Checking Detective



Step	Sift Action	Task / Question	Tool Needed
1. The Emotion Check	Stop	What emotion did the post trigger? Strong emotion = caution.	Self-reflection
2. The Reputation Check	Investigate	Search "[Account/Website] Wikipedia" or "[Name] bias." What do reliable sources say?	Google / Wikipedia
3. The Reality Check	Find	Search the claim in Google News. Are reputable outlets reporting it?	Google News / Snopes
4. The Context Check	Trace	Reverse image search the main image. When and where was it originally used?	Google Lens / TinEye
5. The Verdict	Decision	Is it true, false, or misleading? Will you share, ignore, or report it?	Judgment

09

Cyberbullying Prevention

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

A. Theoretical Knowledge & Critical Understanding

This module empowers youth workers to guide young people (aged 16-25, particularly migrants, refugees, and those from disadvantaged backgrounds) in recognizing, preventing, and stopping cyberbullying. It moves beyond the victim-narrative to focus on bystander intervention and the psychological mechanisms that drive online aggression.
This module addresses the increasing awareness of risks and promotes responsible use by fostering a culture of "Upstanders" who refuse to tolerate digital harassment.

The Online Disinhibition Effect
People behave differently online than face-to-face. The Online Disinhibition Effect explains why.

Dissociative Anonymity ("You Don't Know Me")
Aggressors separate their online actions from their real identity, reducing accountability.

Invisibility ("You Can't See Me")
Without seeing the victim's emotional reaction, empathy is weakened and cruelty escalates.

Solipsistic Introjection ("It's All in My Head")
Without visual cues, aggressors imagine the victim as a villain, justifying harsher behavior.

The Bystander Effect and Pluralistic Ignorance
Cyberbullying is often witnessed by hundreds of peers. Diffusion of Responsibility: Everyone assumes someone else will intervene—so no one does. Pluralistic Ignorance: Bystanders privately disapprove but stay silent because they think others approve. The Audience Effect: Bullies perform for validation. Likes, shares, and even angry comments fuel the behavior. Silence or disapproval removes the reward.

Theoretical Explanation: The Psychology of Online Aggression
Cyberbullying is often mistakenly viewed as simply "bullying that happens on a screen." However, it possesses unique characteristics—anonymity, infinite reach, and permanence—that can make it more psychologically damaging than traditional offline harassment. To prevent it, youth workers must understand the underlying human behaviors that technology amplifies.

Defining Cyberbullying in the Algorithm Age
Traditional bullying relies on physical or social power imbalances. Cyberbullying relies on digital power imbalances.

Repetitive Aggression
Cyberbullying involves repeated, intentional harm delivered through digital devices.

The "Always-On" Phenomenon
Unlike offline bullying, cyberbullying follows the victim everywhere—into their home, their bedroom, and their private spaces. This creates chronic stress and hyper-vigilance.

Digital Power Dynamics
A bully's power may come from:

Technical Skill: hacking, doxxing, photo manipulation

Anonymity: hiding identity to avoid consequences

Social Capital: mobilizing followers to "pile on"

The Typology of Digital Harassment
Cyberbullying takes many forms, each requiring different responses:

Doxing: Releasing private information
Exclusion: Removing someone from group chats or servers
Fraping (Impersonation): Posting from someone's account
Catfishing/Masquerading: Using fake identities to deceive or humiliate

Identity-Based Bullying and the Migrant Experience
For the target group of this project, cyberbullying often intersects with racism and xenophobia, creating Identity-Based Bullying.

Double Victimization: Migrant youth often face exclusion in the "real world" due to language or cultural barriers. When this exclusion follows them online (where they hoped to find a connection), the psychological impact is compounded.

The "Forever Foreigner" Syndrome: Online harassment often attacks the victim's core identity (religion, accent, origin), reinforcing the message that they do not belong. Unlike behavioral bullying (which stops if behavior changes), identity bullying attacks who the person is, making them feel helpless.

B. Practical Guidance: The 5Ds of Bystander Intervention

The goal of this section is to transform passive bystanders into active "Upstanders." Research shows that when peers intervene, bullying stops within 10 seconds in 57% of cases. However, youth often fear becoming the next target. Therefore, the strategies below prioritize safety and options over direct heroics.
We utilize the 5Ds Methodology (developed by Right To Be), which provides a spectrum of intervention styles ranging from subtle to direct.

The 5Ds of Bystander Intervention

1. DISTRACT (The Subtle Interruption)
Goal: To derail the incident without confronting the bully directly. This de-escalates the situation by breaking the "mob mentality" focus.
When to use: When you feel unsafe confronting the aggressor, or when the bullying is happening in a public group chat.

Tactics:
The Subject Change: "Hey guys, has anyone seen the homework assignment? I'm totally lost."
The Meme Flood: "Omg look at this cat video I just found." (Encourage others to post random things to bury the mean comments).
The Shared Interest: Tag the victim in a conversation about a shared hobby: "@[Victim], are you still playing [Game]? I need a teammate."

2. DELEGATE (Asking for Backup)
Goal: To bring in a third party who has more authority or ability to handle the situation.
When to use: When there is a threat of physical violence, "doxing" (release of private info), or when you feel overwhelmed.

Tactics:
Platform Mods: On Discord or Twitch, message a moderator: "User X is breaking the rules in the general chat."
Trusted Adults: If it involves classmates, screenshot the evidence and show a teacher or youth worker.
The "Friend Check": Message another friend privately: "Hey, look at what's happening in the group chat. Should we both say something?" (Strength in numbers).

3. DOCUMENT (Evidence Collection)
Goal: To preserve proof of the harassment for future reporting. Cyberbullying evidence is fragile; posts can be deleted in seconds.
When to use: ALWAYS. Before reporting or blocking, you must document.

Tactics:
The Full Screenshot: Capture the entire screen, including the date, time, URL (if applicable), and the profile of the bully.
Do Not Respond: Taking the screenshot should be done silently. Do not warn the bully ("I'm screenshotting this!"), as they may block you or delete the evidence immediately.
Safe Storage: Save these images in a specific folder, not just the camera roll.

4. DELAY (Support After the Fact)
Goal: To support the victim after the incident has occurred. This is often the most powerful intervention because it breaks the victim's isolation.
When to use: When you were unable to act in the moment, or when the bullying happened publicly, and you want to show support privately.

Tactics:
The Check-In: Send a private DM: "Hey, I saw what they posted. It was really uncool and not true. Are you doing okay?"
Validation: Remind them: "You don't deserve that. They are just trying to get a reaction."
Distraction: "Do you want to get off this app and go play a game/grab food?"

5. DIRECT (Setting the Boundary)
Goal: To stop the behavior by naming it. This carries the highest risk of retaliation, so it must be done carefully.
When to use: When you feel safe, physically and socially, and you believe the aggressor might listen.

Tactics:
Keep it Short: Do not argue. Do not insult the bully back (this fuels them).
The Pivot: "That's not funny." / "We don't do that here." / "Leave him alone."
The "I" Statement: "I don't like how this conversation is going. I'm muting this chat."

Technical Self-Defense: The Digital Shield
Youth workers must teach the technical difference between Blocking, Muting, and Reporting.

Blocking: Stops contact but may escalate retaliation

Muting/Restricting: Silently hides the bully's comments from others

Reporting
Use specific categories (e.g., "Hate Speech") for stronger platform action.

III. Real-Life Examples

1. Fraping & Impersonation — The Megan Meier Case
A fake profile created by an adult led to a teenager's death, prompting global legal reforms.

2. Identity-Based Bullying — The Jamal Hijazi Case
A Syrian refugee was assaulted and then targeted by online disinformation campaigns.

3. Doxing & Swatting — The Wichita Case
A gaming dispute escalated into a fatal police encounter; the perpetrator received a 20-year sentence.

IV. Practical Worksheet: The Upstander's Action Plan

Target Audience:
Youth (16-25) guided by a Youth Worker.

Activity Goal:
To move from "passive witnessing" to "active intervention." By pre-scripting responses, youth reduce the fear of not knowing what to say in the heat of the moment.

Part 1: The 5D Scenario Drill
Instruction: Read the specific scenario in the left column. Choose one of the "5Ds" (Distract, Delegate, Document, Delay, Direct) that feels safest to you. Then, write down exactly what you would do or say.

Scenario	Strategy (Pick a D)	Your Script / Action Plan	Why This Works
Classmate posts embarrassing photo; group laughs	DISTRACT	Flood chat with new topic or meme	Breaks mob momentum
Hate speech comment on friend's TikTok	DOCUMENT & DELEGATE	Screenshot → Report → Support friend	Stops algorithmic amplification
Friend excluded from Discord	DELAY	DM: "I noticed you weren't there today—want to play together?"	Counters isolation
Doxing threat	DELEGATE	Screenshot → Show adult immediately	Safety risk requires authority
"Prank" impersonation	DIRECT	Script: "That's not funny."	Sets boundary without escalation

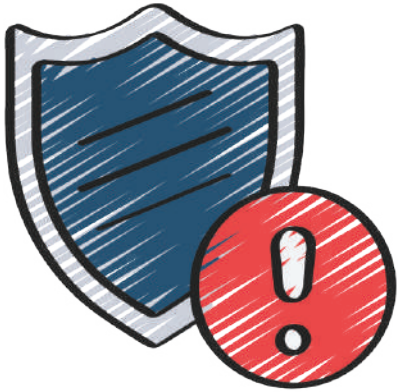
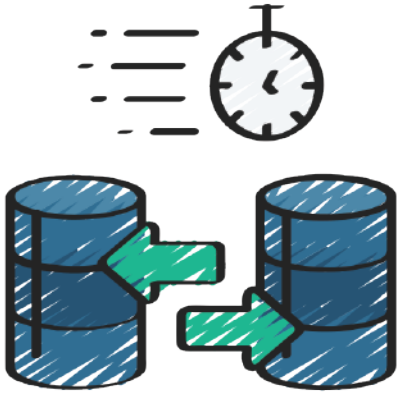
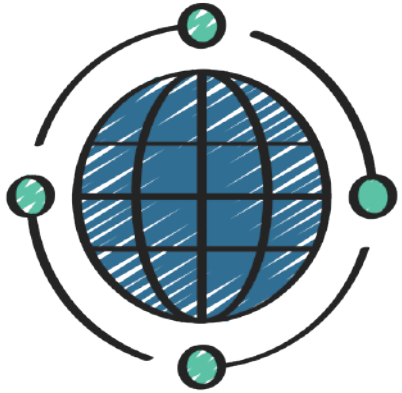
Part 2: The "Digital Shield" Audit
Instruction: Cyberbullying prevention is also technical. Open your primary social media app (Instagram, TikTok, or Snapchat) and complete this checklist to "harden" your defenses.

[ ] 1. The "Tagging" Lock
Action: Go to Settings > Privacy > Tags/Mentions.
Setting: Change "Allow tags from" to "People you follow" or enable "Manually Approve Tags."
Why: This prevents bullies from tagging you in humiliating posts that then appear on your own profile.

[ ] 2. The "Mute" Strategy
Action: Identify one account that annoys you or posts mean comments, but you are afraid to block (to avoid drama).
Setting: Select "Restrict" (Instagram) or "Mute" (Twitter/IG).
Why: They can still comment, but only they see it. You stop seeing their content, protecting your mental health without alerting them.

[ ] 3. The "Evidence" Vault
Action: Create a folder on your phone or cloud drive named "Receipts" (or something boring like "Notes").
Strategy: If harassment starts, screenshot everything to this folder immediately. Even if you don't report it today, having a timeline of evidence is crucial if it escalates to legal or school authorities later.

Part 3: The Safety Check (Self-Reflection)
Before intervening, always ask yourself the "3 Safety Questions." If the answer is NO, use "Delegate" (get help) instead of acting alone.
1. Am I physically safe? (Is this person in the same room/school as me? Are they violent?)
2. Am I socially safe? (Do I have friends who will back me up, or am I acting entirely alone?)
3. Am I emotionally ready? (Do I have the energy to deal with the potential backlash today?).

10

Digital Footprints

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

Mastering Your Online Legacy

This module empowers youth workers to guide young people (aged 16–25) in understanding that every interaction online leaves a trace. It shifts the narrative from "hiding" to "curating," teaching youth how to manage their data trail to protect their privacy, ensure their safety, and build a positive digital reputation that opens doors rather than closing them.

This module addresses digital readiness and safety by revealing the invisible mechanisms of data tracking and the long-term consequences of online actions.

I. Theoretical Explanation: The Anatomy of Data Trails

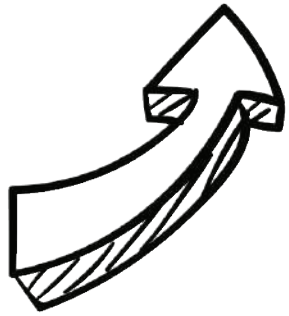
To navigate the digital world safely, youth must understand that a "Digital Footprint" is not just a collection of old photos; it is a dynamic, monetizable, and permanent asset that defines their identity in the eyes of algorithms, employers, and governments.

Active Digital Footprint (The "Performance")
Definition:
Data that a user intentionally creates and submits. This is the "curated self"—the version of their life they want the world to see.

Examples:
Posting a photo on Instagram, writing a tweet, sending an email, filling out an online form.

The Illusion of Control:
Users often feel they control this footprint because they hit "publish."
However, once posted, control is lost due to screenshots, resharing, and archiving.

Passive Digital Footprint (The "Shadow")
Definition:
Data collected about a user without their active creation, often invisibly. This is the "quantified self"—the behavioral reality of who they are.



Mechanisms:
Tracking technologies such as:
HTTP Cookies, Device Fingerprinting, Beacons

Examples:

Metadata: EXIF data in photos (camera model, date, GPS coordinates)

Clickstream Data: Hover time, abandoned carts, browsing time of day

2. The Mosaic Effect and Data Aggregation

The greatest risk to digital privacy is not a single data leak, but the Mosaic Effect—when harmless data points combine to reveal sensitive information.

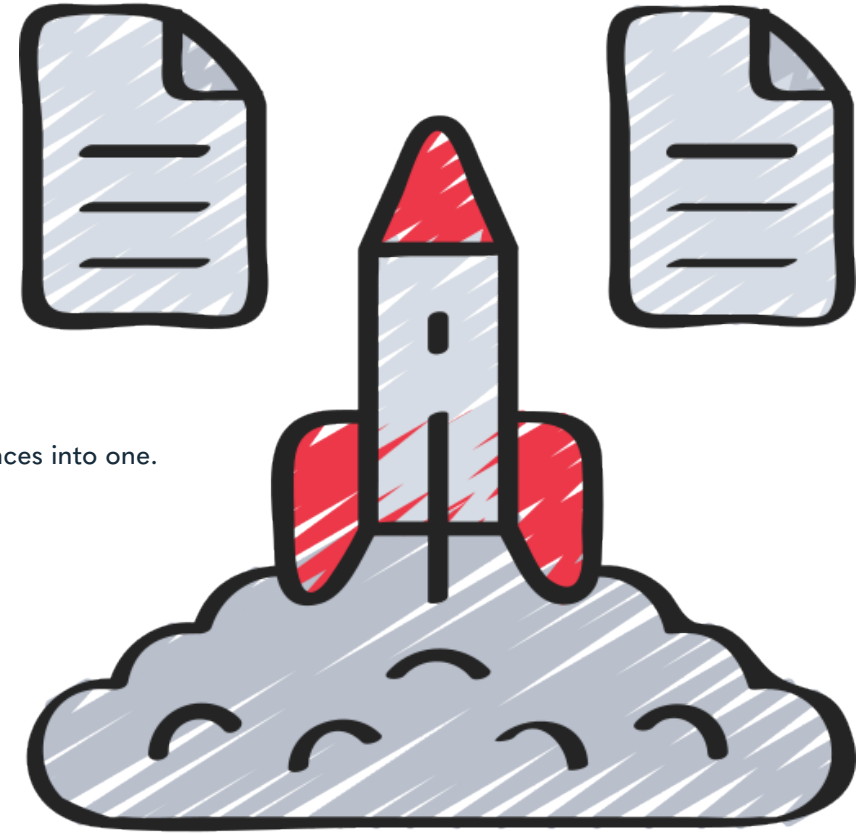
Data Aggregation
Data brokers scrape: Public records, Social media bios, Shopping histories

Inference
Algorithms analyze aggregated data to make predictions.

Example:
Unscented lotion + vitamin subscription + classical music playlist →
Algorithm infers pregnancy before the user tells their family.

Relevance to Migrants/Refugees
Data points like: Language settings, Money transfer apps, Location history

...can reveal migration routes or legal vulnerabilities.



3. Context Collapse and the "Invisible Audience"

Sociologist Danah Boyd describes Context Collapse as the flattening of multiple audiences into one.

The Problem
Offline, we separate audiences (grandmother, boss, best friend).
Online, one post may reach all of them simultaneously.

The Consequence
A joke meant for close friends may be misinterpreted by a future employer.

The Invisible Audience
Users imagine "my friends," but forget:

Algorithms, Archivists, Law enforcement, Recruiters

This cognitive gap leads to oversharing.

4. The Economy of Reputation: The "Long Tail" of Data

The internet operates on server time, not human time.

Archival Persistence
Deleted posts may survive in:
Server backups

The Wayback Machine
Screenshots, The Vetting Machine
Digital footprints are now primary vetting tools.

Employment: 77% of recruiters screen candidates online

Universities: Admissions officers check digital behavior

Visa authorities: Increasingly assess "character" through digital history

A careless footprint can restrict opportunities. A "ghost" (no footprint) is also suspicious.

II. Practical Guidance: The Digital Audit and Curation Strategy

Managing a digital footprint requires both defensive and offensive strategies.
Youth workers can guide participants using the Audit → Clean → Curate framework.

1. The Defensive Audit: "Ego-Surfing" Like a Pro
Most youth think they know what's online about them—but search engines personalize results.

The Incognito Necessity Why: Regular searches show personalized results.

Action: Use Incognito/Private mode to simulate a stranger's view.

The Deep Dive Checklist

Web Search: Search name + city + school. Check first 5 pages.
Image Search: Look for old photos, tagged images, forgotten accounts.
Handle Search: Search usernames used across platforms. Employers and data brokers connect these easily.

2. Managing the Passive Footprint: Metadata and Permissions

The Location Lockdown
Risk: Apps request precise location unnecessarily.

Action: Set permissions to "While Using App" or "Never."

The EXIF Trap
Risk: Photos contain GPS coordinates when shared via email, SMS, Discord.

Action: Warn youth that sending a selfie can reveal their home address.

III. Real-Life Examples

These cases illustrate:
Context Collapse, Passive Data Risks, Positive Curation

Example 1: Harvard Rescinded Offers (Context Collapse)

Event:
Harvard revoked offers to 10 admitted students.

Cause:
Offensive memes shared in a "private" Facebook group.

Lesson:
There is no such thing as private online spaces.
Institutions judge digital behavior as character.

Example 2: The Strava Heatmap (Passive Footprint Risk)

Event:
Strava's global heatmap revealed secret military bases.

Cause:
Passive GPS data from soldiers' fitness routines.

Lesson:
You don't need to post to leave a footprint.

3. The Active Cleanup: Scrubbing History

Use the Billboard Test:
"If this post were on a billboard outside my future boss's office, would I get the job?"

Delete vs. Archive
Delete: Offensive, illegal, harmful content
Archive: Personal or "cringe" content

The "Ghost Account" Problem
Old accounts = security risks.

4. The Offensive Strategy: SEO Curation
A clean footprint is not enough. Youth must build a positive footprint.

SEO for Humans
Goal: Push positive content to page 1 of Google.

Action: Create professional profiles on:

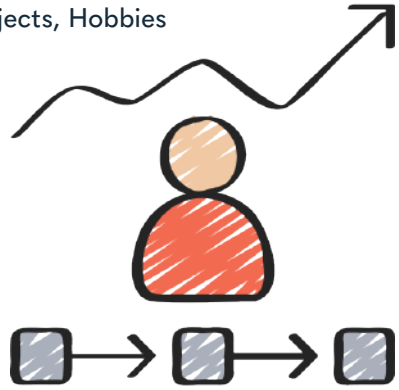
LinkedIn, Behance, Medium

These have high domain authority.

Green Flags
Encourage youth to post:

Volunteer work, Certificates, Creative projects, Hobbies

This turns the footprint into a portfolio.



IV. Practical Worksheet: The Footprint Forensics Lab

Part 1: The Search Engine Audit
Use Incognito mode.

Checklist:

[ ] Does your home address appear

[ ] Old accounts visible

[ ] Do images represent who you are today

Part 2: The "Cookie Monster" Check
Observe targeted ads for 24 hours.

Reflection:

What ads follow you

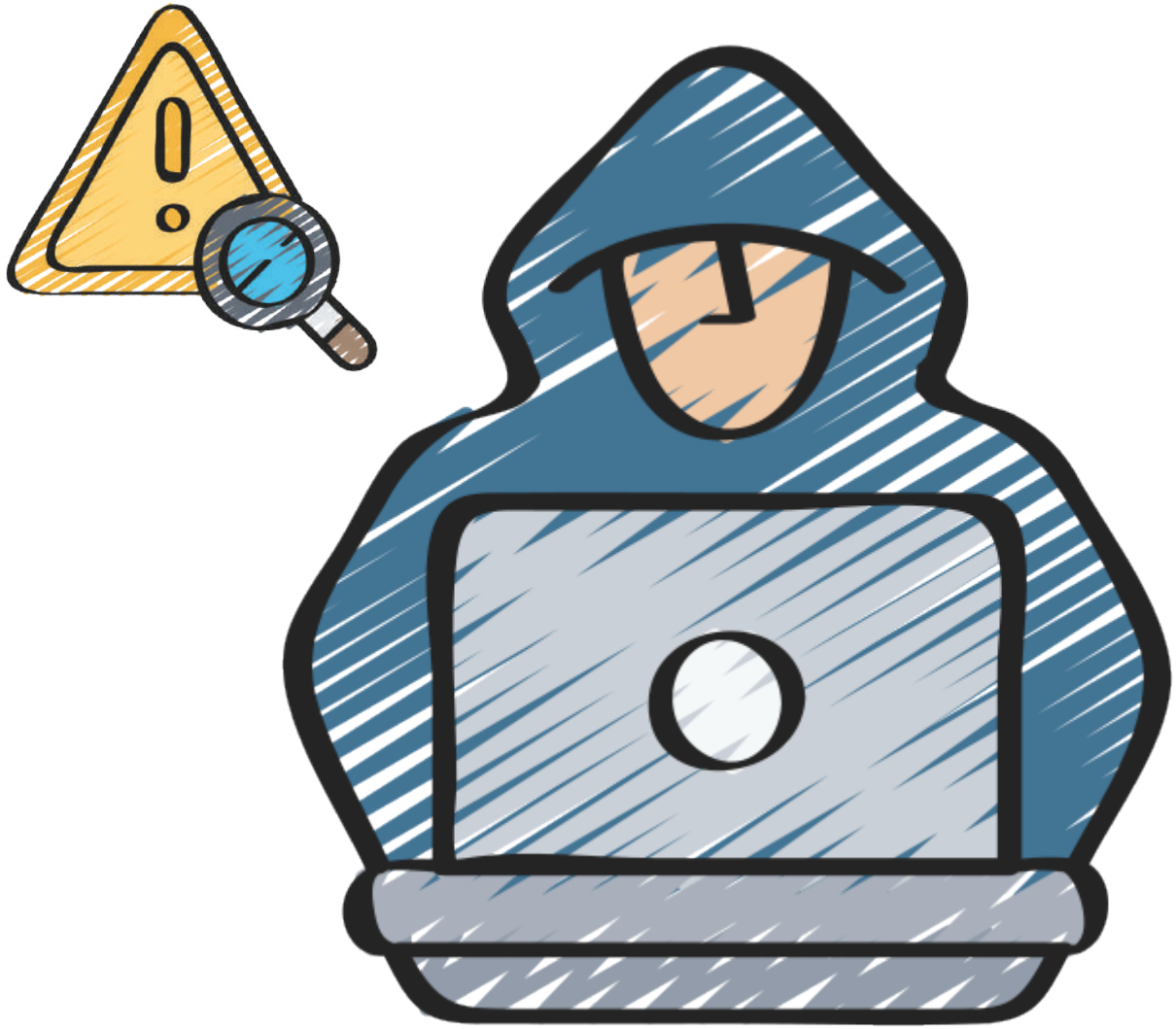
What does the algorithm infer about you

Part 3: The App Permission Cleanup
Check:

Microphone permissions

Location permissions

Ask:
"Does this app really need this access?"



11 Conclusion

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

The EthiTech Toolkit concludes not as a final destination, but as a launchpad for continuous digital engagement. Throughout these modules, we have moved beyond the traditional, limited narrative of "internet safety"—which focuses primarily on avoidance and fear—toward a holistic vision of Digital Citizenship. This vision defines the digital world not merely as a risk to be managed, but as a community to be built, a marketplace to be navigated, and a stage for empowered self-expression.

1. Synthesizing the Core Framework: Safe, Savvy, Social
At the heart of this toolkit lies the S3 Framework, which simplifies complex digital behaviors into actionable habits for daily life.

Safe (Protect): We have established that safety is active, not passive. From "hardening" our devices against social engineering to understanding the invisible "passive footprint" of metadata and cookies, participants are now equipped to lock down their digital lives.

Savvy (Educate): We have transitioned from passive consumption to critical inquiry. By applying the SIFT method (Stop, Investigate, Find, Trace) and understanding the "Attention Economy", learners can now navigate the "Information Disorder" without falling prey to filter bubbles or polarization.

Social (Respect): We have redefined online interaction through the lens of empathy. By recognizing the "Online Disinhibition Effect" and adopting the "Upstander" mentality against cyberbullying, we foster a digital culture where integrity is maintained even when no one is watching.

2. The Imperative of Inclusion and Employability
A central mission of the EthiTech project is to close the "Digital Divide" that disproportionately affects migrants, refugees, and youth from disadvantaged backgrounds.

Bridging the Gap: This toolkit asserts that functional digital skills—such as secure communication and data literacy—are essential bridges for social and economic inclusion.

From Consumer to Creator: We have shifted the focus from merely scrolling to "Meaningful Creation". By mastering digital storytelling and creative tools, young people can reclaim their narratives, turning their unique lived experiences into assets for advocacy and identity formation.

Future-Proofing: We recognize that a digital footprint is a permanent resume. By teaching youth to "curate" rather than "hide," we transform their online presence into a portfolio that signals employability and entrepreneurial mindset to future gatekeepers.

3. The Ripple Effect: A Call to Action for Youth Workers
For the facilitators, educators, and youth workers (Target Group T2) using this resource, the conclusion of this toolkit marks the beginning of your responsibility. You are the "Digital Mentors" capable of breaking the cycle of toxicity and misinformation.

By implementing the "Train the Trainer" model, you create a ripple effect. Every young person you teach to pause and "THINK" (True, Helpful, Inspiring, Necessary, Kind) before posting or to intervene as an active bystander, contributes to a safer, more democratic, and more inclusive digital society.

Final Takeaway: The digital world is permanent, but it is not fixed; it is shaped by every click, share, and comment we make. The EthiTech Toolkit empowers the next generation to stop being passive inhabitants of the internet and start being its active, ethical architects.

12

Contacts

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

YOUTH WITHOUT BARRIERS

Maastricht, Netherlands
youthwithoutbarriersnl@gmail.com
https://www.instagram.com/ywb_nl/

YCDA

Romania, Piteşti
Contacts: associatiaycd@gmail.com
https://www.instagram.com/ycda.ro/

Jugendvision e.V

Germany, Stuttgart
Contacts: jugendvisionev@gmail.com
https://www.instagram.com/jugendvision.ev/

Türkiye, Ankara
Contacts: info@argusteknoloji.com
https://www.instagram.com/argustechnology/

13

References

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

United Nations Development Programme. (n.d.). Equipping Türkiye's youth with digital skills for tomorrow's jobs.
https://www.undp.org/turkiye/press-releases/equipping-turkiyes-youth-digital-skills-tomorrows-jobs

United Nations Development Programme. (n.d.). 45 digital youth centers opened to prepare young people for future professions.
https://www.undp.org/turkiye/press-releases/45-digital-youth-centers-opened-prepare-young-people-future-professions

United Nations Development Programme. (2024). Today's youth report – Mapping analysis.
https://www.undp.org/sites/g/files/zskgke326/files/2024-12/undp-tr-todays-youth-rapor_04_haritalamaanalizi.pdf

Gülnar, M. (2023). Dijital içerikli eğitimin yetişkinlerin dijital becerilerine etkisi. Akademik Açı.
https://dergipark.org.tr/tr/pub/akademikaci/issue/77112/1268803

Social Sciences Studies Journal. (n.d.). Makale PDF.
https://sssjournal.com/files/sssjournal/2d1fa728-f99a-4af9-9a70-bf3365f22c27.pdf

ERIC. (n.d.). Full-text education article.
https://files.eric.ed.gov/fulltext/EJ1413561.pdf

DergiPark. (n.d.). Makale PDF.
https://dergipark.org.tr/en/download/article-file/2567213

DergiPark. (n.d.). Makale PDF.
https://dergipark.org.tr/tr/download/article-file/1626539

DergiPark. (n.d.). Makale PDF.
https://dergipark.org.tr/tr/download/article-file/2372372

İktisadi Kalkınma Vakfı. (n.d.). Avrupa Birliği'nde dijital eğitim ve becerilerin geliştirilmesi ve Türkiye.
https://www.ikv.org.tr/images/files/ikv_avrupa_birliginde_dijital_egitim%20ve_becerilerin_gelistirilmesi_ve_turkiye_bared_cil.pdf

UNESCO. (n.d.). Digital competencies and skills.
https://www.unesco.org/en/digital-competencies-skills

Özgür Publications. (n.d.). Article with DOI.
https://doi.org/10.58830/ozgur.pub686.c2893

Milli Eğitim Bakanlığı. (2025). Dijital içerik nedir?
https://manavgatfsm.meb.k12.tr/meb_iys_dosyalar/07/12/762114/dosyalar/2025_04/14094756_dcenedir1.pdf

UNESCO. (n.d.). Correcting media myths about refugees and migrants.
https://www.unesco.org/en/articles/correcting-media-myths-about-refugees-and-migrants

American Psychological Association. (n.d.). Bystander intervention.
https://www.apa.org/pi/health-equity/bystander-intervention

eSafety Commissioner. (n.d.). Be an upstander.
https://www.esafety.gov.au/young-people/be-an-upstander

eSafety Commissioner. (n.d.). Digital reputation – Staying safe.
https://www.esafety.gov.au/key-topics/staying-safe/digital-reputation

European Commission. (n.d.). Cyberbullying policy.
https://digital-strategy.ec.europa.eu/en/policies/cyberbullying

Gámez-Guadix, M., et al. (2021). [Article in Frontiers in Psychology].
https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.676787/full

MDPI. (n.d.). Social Sciences article.
https://www.mdpi.com/2076-0760/13/1/64

Right To Be. (n.d.). Bystander intervention training.
https://righttobe.org/guides/bystander-intervention-training/

Securly. (n.d.). The 10 types of cyberbullying.
https://blog.securly.com/the-10-types-of-cyberbullying/

U.S. Department of Health & Human Services. (n.d.). Cyberbullying guide.
https://www.stopbullying.gov/sites/default/files/documents/Cyberbullying%20Guide%20Final%20508.pdf

Safer Internet UK. (n.d.). Cyberbullying: Practical advice for professionals.
https://saferinternet.org.uk/guide-and-resource/cyberbullying-practical-advice-for-professionals-working-with-young-people

UNICEF. (n.d.). How to stop cyberbullying.
https://www.unicef.org/stories/how-to-stop-cyberbullying

Internet Society. (n.d.). Digital footprints.
https://www.internetsociety.org/learning/digital-footprints/

Council of Europe. (n.d.). Digital citizenship education.
https://www.coe.int/en/web/digital-citizenship-education

Council of Europe. (n.d.). Easy steps to help your child become a digital citizen.
https://rm.coe.int/easy-steps-to-help-your-child-become-a-digital-citizen/16809e2d1d

Edutopia. (n.d.). Teacher's guide to copyright and fair use.
https://www.edutopia.org/article/teachers-guide-copyright-and-fair-use/

Edutopia. (n.d.). 10 visual literacy strategies.
https://www.edutopia.org/blog/ccia-10-visual-literacy-strategies-todd-finley

Canadian Centre for Cyber Security. (n.d.). Digital footprint guidance (ITSAP00133).
https://www.cyber.gc.ca/en/guidance/digital-footprint-itsap00133

Common Sense Education. (n.d.). Digital citizenship.
https://www.commonsense.org/education/digital-citizenship

Child Mind Institute. (n.d.). How using social media affects teenagers.
https://childmind.org/article/how-using-social-media-affects-teenagers/

Childnet. (n.d.). Online reputation guidance.
https://www.childnet.com/help-and-advice/online-reputation/

CyberSmarties. (n.d.). Behind the screen: How algorithms shape what kids see online.
https://cybersmarties.com/behind-the-screen-how-algorithms-shape-what-kids-see-online/

Johns Hopkins Medicine. (n.d.). Social media and mental health in children and teens.
https://www.hopkinsmedicine.org/health/wellness-and-prevention/social-media-and-mental-health-in-children-and-teens

PubMed Central. (n.d.). Open-access article.
https://pmc.ncbi.nlm.nih.gov/articles/PMC12356748/

Verizon. (n.d.). Retrain your social media algorithm.
https://www.verizon.com/about/parenting/retrain-social-media-algorithm

Verizon. (n.d.). How to be a guardian for your kid's online identity.
https://www.verizon.com/about/parenting/how-to-be-a-guardian-for-your-kids-online-identity

Digital Child. (n.d.). Ethical considerations in research on digital childhoods.
https://digitalchild.org.au/research/publications/working-paper/ethical-considerations-in-research-on-digital-childhoods/

Finley, T. (n.d.). 10 visual literacy strategies. Edutopia.
https://www.edutopia.org/blog/ccia-10-visual-literacy-strategies-todd-finley

GurkhaTech. (n.d.). Short-form video storytelling guide.
https://gurkhatech.com/short-form-video-storytelling-guide/

Wake Forest University. (2016). Seven elements of digital storytelling.
https://prod.wp.cdn.aws.wfu.edu/sites/18/2016/03/Seven-Elements-of-Digital-Storytelling-Handout.pdf

AME Publishing Company. (n.d.). mHealth article.
https://mhealth.amegroups.org/article/view/140462/html

UNICEF. (n.d.). Reporting guidelines.
https://www.unicef.org/media/reporting-guidelines

Future of Privacy Forum. (2018). GDPR–CCPA comparison guide.
https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf

Springer. (n.d.). Book chapter.
https://link.springer.com/chapter/10.1007/978-3-031-46929-9_15

Nature. (2023). Scientific article.
https://www.nature.com/articles/s41599-023-02501-4

KVKK. (n.d.). Kişisel verilerin korunması rehberi.
https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/13711235-abb6-4b17-9a6b-0a68c1ad86c5.pdf

Kaspersky. (n.d.). Top 10 preemptive safety rules.
https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online

Socrates Journal. (n.d.). Makale.
https://socratesjournal.org/index.php/pub/article/view/515

DergiPark. (n.d.). Makale PDF.
https://dergipark.org.tr/en/download/article-file/2567213

14 Appendices

Fostering Responsible Digital Citizenship in Youth Erasmus+ Small-scale Partnerships in the Field of Youth

2023-3-NL02-KA210-YOU-000178752

Appendix A: Glossary of Key Terms

Active Digital Footprint: Data that a user intentionally creates and submits, such as social media posts, comments, emails, or uploaded photos.
Context Collapse: A phenomenon where multiple distinct audiences (e.g., friends, family, employers) are flattened into a single audience on social media, often leading to misunderstandings when content intended for one group is viewed by another.

Digital Citizenship: The norm of appropriate, responsible, and empowered technology use, organized under the principles of Respect, Educate, and Protect.
Digital Divide: The gap between those who have access to modern information and communication technology (and the skills to use it) and those who do not, often exacerbating social and economic inequality.

Doxing: The public release of private, identifiable information (such as a home address or phone number) without the owner's consent, often used to intimidate or endanger the victim.
Filter Bubble: A state of intellectual isolation that results from algorithms guessing what information a user would like to see based on their past behavior, thereby separating them from information that disagrees with their viewpoints.

Information Disorder: A framework that categorizes false or harmful information into three types: Misinformation (false connection/context without intent to harm), Disinformation (intentional fabrication to cause harm), and Malinformation (genuine information shared publicly to cause harm).
Mosaic Effect: The process by which disparate, seemingly harmless pieces of data (e.g., a playlist change + a purchase history) are aggregated to reveal sensitive private information.

Online Disinhibition Effect: The psychological phenomenon where people behave differently online—sometimes more openly or more aggressively—due to perceived anonymity and lack of real-time eye contact.
Passive Digital Footprint: Data collected about a user without their active creation, such as IP addresses, browsing history, device location, and metadata.

Phishing: A form of social engineering where attackers use fake emails or websites to deceive individuals into disclosing sensitive information like login credentials.
Social Engineering: The exploitation of human psychology (rather than technical hacking) to gain unauthorized access to sensitive information.
Synthetic Media (Deepfakes): Media generated or manipulated by artificial intelligence, such as swapping faces or cloning voices, are often used to create convincing but false evidence.

Appendix B: Core Frameworks & Methodologies

1. The S3 Framework (Digital Citizenship Model)
A simplified model for daily digital application:
Safe (Protect): Focusing on security, privacy, and health (e.g., using strong passwords, recognizing addiction).
Savvy (Educate): Focusing on literacy, commerce, and law (e.g., spotting fake news, understanding copyright).
Social (Respect): Focusing on etiquette, access, and rights (e.g., respecting others, closing the digital divide).

2. The THINK Method (Content Posting Filter)
A reflective acronym to combat impulsive posting:
T = Is it True? (Have you verified the source?)
H = Is it Helpful? (Does it add value or merely noise?)
I = Is it Inspiring? (Does it reflect your best digital self?)
N = Is it Necessary? (Is this better discussed in private?)
K = Is it Kind? (Would you be okay with a grandmother reading this?)

3. The SIFT Method (Verification Strategy)
A four-step process for analyzing information credibility:
Stop: Check your emotions. If a post triggers anger or shock, pause before sharing.
Investigate the Source: Don't just look at the "About Us" page; search outside the site to see what others say about it.
Find Better Coverage: Look for the same story in multiple reputable news outlets.
Trace Claims: Find the original context of the quote, image, or study to ensure it hasn't been stripped of meaning.

4. The 5Ds of Bystander Intervention (Anti-Cyberbullying)
Strategies to intervene safely when witnessing online harassment:
Distract: Derail the incident subtly (e.g., posting a meme or changing the subject).
Delegate: Ask for help from a third party (moderator, teacher, or another friend).
Document: Screenshot the evidence safely (without notifying the aggressor) for future reporting.
Delay: Check in with the victim after the incident to offer support.
Direct: Set a boundary by confronting the behavior directly (only if physically/socially safe).

Appendix C: Index of Practical Worksheets

Worksheet Title	Module Reference	Purpose
Digital Tool Inventory & Skills Gap Assessment	Module 2	For youth workers to assess their own digital functional skills and training needs.
The Digital Safety Audit	Module 3	A checklist for implementing MFA, Password Managers, and checking device hygiene.
The S3 Digital Health Check	Module 4	A self-assessment scale (1-5) for youth to rate their habits in Safety, Literacy, and Etiquette.
The "Feelings & Options" Dilemma Solver	Module 5	A structured guide for resolving online ethical conflicts (identifying victims, imagining options).
The Social Media Audit	Module 6	A step-by-step guide to cleaning up feeds, adjusting privacy, and "retraining" algorithms.
The Digital Story Canvas	Module 7	A planning grid for digital storytelling, covering the Core Message, Hook, Voice, and Safety Check.
The Fact-Checking Detective	Module 8	A template for applying the SIFT method to a specific piece of suspect content.
The Upstander's Action Plan	Module 9	A scenario drill where youth script their responses to bullying using the 5Ds.
The Footprint Forensics Lab	Module 10	An activity guide for performing a "Clean Search" (Incognito) and auditing app permissions.

Appendix D: Recommended Digital Tools

Security & Privacy:

Password Managers: Essential for maintaining unique, strong passwords.

VPNs (Virtual Private Networks): Recommended for securing data when using public Wi-Fi.

JustDelete.me: A directory of direct links to permanently delete unused online accounts.

Verification & Fact-Checking:

Google Lens / TinEye / Yandex Images: For reverse image searching to verify visual content.

Snopes.com: For cross-referencing viral stories and urban legends.

Wikipedia: For checking the reputation and bias of media outlets.

Creativity & Collaboration:

Canva / CapCut: Accessible tools for mobile-friendly content creation and video editing.

Miro / Jamboard: Collaborative digital whiteboards for brainstorming and group work.

Actionbound: For creating gamified, location-based learning quests.

Co-funded by the European Union

Co-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 Nederlands Jeugdinstituut. Neither the European Union nor the National Agency can be held responsible for them.