

Digital

Literacy

</forum

DLF MODULES

Digital Literacy Toolkit



American Spaces

Table of Contents

INTRODUCTION TO THE TOOLKIT	2
MEDIA & DIGITAL LITERACY	4
MODULE ICE BREAKER	7
MINI LESSON: STUDENT-GENERATED STORY	8
MINI LESSON: HOW TO CREATE “UNCRACKABLE” PASSWORDS	12
MINI LESSON: DIGITAL FOOTPRINT	14
MINI LESSON: BE A VILLAIN	17
MODULE WRAP-UP: PERSONAL DIGITAL SAFETY PLEDGE	19
UNDERSTANDING SOCIAL MEDIA ALGORITHMS	20
MINI LESSON: GOING DEEPER INTO SOCIAL MEDIA ALGORITHMS	25
MINI LESSON: EFFECTS OF ALGORITHMS ON YOUNG PEOPLE	30
ONLINE BEHAVIOR	33
MINI LESSON: HUMAN RIGHTS ONLINE	34
MINI LESSON: ONLINE VIOLENCE/HATE SPEECH	40
MINI LESSON: CYBERBULLYING	44
MINI LESSON: CANCEL CULTURE	48
MINI LESSON: DEEPPFAKE TECHNOLOGY	61

Introduction to the Toolkit

Welcome to the *Digital Literacy Toolkit*, developed within the Digital Literacy Forum (DLF) project, an American Spaces regional initiative organized by the Regional Public Engagement Specialist (REPS) Office in Belgrade and the U.S. Embassy Tirana that was held in Tirana, Albania, from May 22nd to 24th, 2024. DLF brought together 40 innovative educators, both formal and informal, from across the Western Balkans, including Albania, Bosnia and Herzegovina, Bulgaria, Kosovo, Montenegro, North Macedonia, Romania, and Serbia. These participants, along with eight distinguished local and international experts, united to tackle the critical challenges and opportunities in digital literacy.

The forum resulted in the creation of the *Digital Literacy Toolkit*, a collection of experiential learning modules specifically designed to engage the youth in American Spaces, as well as other audiences of emerging voices. These modules address essential areas such as digital citizenship, responsible online communication, understanding social media algorithms, and developing future-proofing skills in a technology-driven world. Each module in this Toolkit can be delivered in its entirety or in parts, either independently or in combination with other modules.

The *Digital Literacy Toolkit* is intended as a resource for American Spaces managers, educators, trainers, and community leaders committed to equipping the next generation with the tools and knowledge necessary to thrive in the digital age. By implementing these modules, we aim to empower young people to engage with digital platforms responsibly, critically assess the information they encounter, and contribute to a more informed and ethical digital society.

Special thanks to our trainers, Maja Čalović, Ari Daniel, Prof. Vladimir Trajković, Dr. Carlise Womack Wynne, Martina Bolibruchova, Filip Milošević, Bojana Kostić, and Dr. Adam Maltese, whose expertise and dedication were crucial in shaping the resources. We also express our gratitude to our esteemed lecturer, Dr. Edlira Martiri, for her valuable insights. Additionally, we appreciate our moderators, Monika Hanley and Roden Hoxha, for expertly guiding the conversations and ensuring a productive exchange of ideas.

We extend a special acknowledgment to the 40 participants from across the Balkans, whose active engagement and diverse perspectives were vital in developing the Toolkit. Their contributions enriched the discussions, making the Forum's outcomes collaborative and impactful, and resulting in practical tools for educators globally.

We hope this book not only provides practical tools but also inspires ongoing learning and innovation in the field of digital literacy. Thank you for your commitment to fostering a more digitally literate and responsible society.

MODULE

Media & Digital Literacy

SOCIAL MEDIA MAZE

Theme: Digital safety and media literacy basic concepts

Core Concepts/Overview of Topic:

- Personal data protection
- Data privacy awareness
- Social media privacy settings
- Source verification and fact-checking
- Critical evaluation of content sources, media, and context
- Digital identity and online presence

90–120 minutes (Module Ice Breaker + One Mini Lesson of Choice + Wrap Up)

Description of Target Audience: The workshop is designed for individuals aged 15 to 21 (the ideal age range is 18 to 21, but the content is also suitable for those aged 15 to 18).

We assume that the participants:

- Are digital natives with beginner or intermediate knowledge about media literacy
- Are tech-savvy, using mainly their phones for recreational purposes and sometimes for learning
- Have their passwords saved in their phones, though may not remember the passwords if they need them. Some of them may have had their accounts hacked in the past due to weak passwords

Learning Objectives:

Workshop participants will be able to understand and apply basic principles of digital safety including recognizing weak passwords, creating strong passwords, and using password management tools and two-factor authentication.

Participants will be able to define “a digital footprint” and why personal data protection is important. They will familiarize themselves with data privacy and be able to use social media privacy settings.

Participants will be able to understand how their personal information, if not protected, can be misused, misrepresented and exploited. They will understand the importance of responsible online behavior and develop skills to navigate digital spaces safely.

Definitions:

- Digital identity** is a collection of information about a person that exists online.
- Digital activity** refers to online behavior and its resulting impact.
- Digital safety** refers to protection of personal and sensitive information online from threats like cyberattacks and identity theft

Materials, Supplies, and Technology:

- 1 Each participant should be provided with an envelope and a few pieces of paper
- 2 Internet connection
- 3 Projector to display presentations and interactive content
- 4 Laptops for participants to engage in hands-on activities and access online resources
- 5 Paper and markers for note taking, brainstorming sessions, and interactive exercises
- 6 Mobile phones for some parts of the workshop
- 7 Kahoot account: <https://create.kahoot.it/details/b3403099-79df-40fe-b5d1-f412076915a5>

Prep Work (for the workshop facilitator/teacher)

- 1 Two-factor authentication on Google
(Please check out this video <https://www.youtube.com/watch?v=e3Mph-7kqE1E&t=40s>)
- 2 Tools for password management
(Please check out this video <https://www.youtube.com/watch?v=l8Jjowp-La-Q>)
- 3 Real-world examples of data breaches and their impacts
(Please read the following post <https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html>)

MODULE ICE BREAKER (15–20 MINS)

We suggest starting the workshop with an ice breaker. Here are two suggestions, but feel free to use your own if you prefer.

#1: Two truths and a lie is a great game that creates opportunities for students to connect with each other as they exchange information about themselves. The game's concept is simple, making it ideal for small or large groups. First, invite students to sit or stand in a circle. Each member of the group has to introduce themselves and make three statements about themselves. **Two of the statements should be truths, while the other should be a lie.** The rest of the group has to guess which statement is a lie. The challenge is to guess the lies of others while convincing them of yours. For example:

- 1 I am left-handed like my father
- 2 I have never broken a bone
- 3 I was born in a different country

Everyone takes turns introducing themselves and making their statements. After each student's turn, the other players try to guess which statement is the lie. After everyone is done guessing, the player whose turn it was reveals which statement was the lie. The game continues until everyone has had a turn.

These are simple strategies which can make this game more challenging and enjoyable for everyone involved:

- Keep your two truths and a lie simple and believable
- Change up the order of your truths and lie
- Try to make your truths surprising or something people would not expect from you
- Keep your facial expressions neutral
- Choose diverse topics for your statements
- Make all of your statements confidently
- Do not let your body language give you away

Encourage creativity by asking participants to think of interesting and unique facts. This makes the game more engaging. And be inclusive by making sure everyone feels comfortable participating. If someone is shy, they can pass or pair up with a partner.

This activity is intended to help students get to know each other and improve their skills in distinguishing between accurate information and misinformation (a skill that this workshop will lay out in practical digital contexts as well).

#2: Truth about me is another game that can be played to activate connections. Invite students to stand in a circle. It may be useful to mark each person's space with a small piece of tape or some other floor marker. The teacher stands in the center of the circle and introduces the activity: *One of our goals today is to learn more about each other. In this game, the person in the center will share something about themselves by saying, "The truth about me is..." and then complete the sentence with a true fact. For example, "The truth about me is that I like ice cream." If the statement is true about you – that you like ice cream too – then you must leave your current spot in the circle and find a new place to stand.*

The teacher explains that the person in the middle is also trying to secure a spot, so whichever individual does not get a spot goes to the center and the game begins again with a new truth that they say. The teacher encourages students to choose truths that will get more people to move. If the same person ends up in the center multiple times, they can choose a replacement who has not been in the center yet.

Afterwards, the teacher could ask reflection questions:

- *What did you notice about yourself as you played the game?*
- *What did you notice/learn about the group? Why is this important to know?*

Moving in response to shared truths helps participants gain an awareness of the diversity and commonalities within the group, which can help create empathy. The movement encourages participants to be open and honest: seeing others move in response to the same truth can validate one's own experiences and encourage further sharing.

MINI LESSON: STUDENT-GENERATED STORY (1 HOUR)

The objective of this mini lesson is to create a story that highlights issues related to digital safety and media literacy. It aims to promote critical thinking and problem-solving skills among participants, fostering a deeper understanding and practical knowledge they can apply in their own lives.

Introduction (10 mins) How do students perceive themselves online versus offline? In small groups, students compare and contrast their online profiles (social media, gaming, etc.) with their real life identities.

Creating an online character (20 mins) Through this character, the students will learn about the dangers and impacts of online actions.

As a class, first discuss story structure and the elements of what makes a good story. These ingredients can be found [here](#).

Divide students into small groups again. Each group will work on a segment of the story. For example:

- Group 1: Introduction of the main character and their background, demographic, appearance, personality, skills and abilities, social media accounts, etc.
- Group 2: An incident where the main character experiences a digital safety issue. The consequences of the incident and initial reactions
- Group 3: How the main character seeks help and the steps they take to resolve the issue

Encourage creativity, monitor and assist students as they develop their ideas. This process can take whichever format works best for you and your students. It can be the group work model as we've outlined above, a collective effort, a discussion, or each student can have a different responsibility to figure out a particular aspect of the narrative (e.g., character's name, gender, hair color, age, profession, background, problem, etc.).

At the end, the students work together to combine their ideas into a cohesive narrative. Encourage participants to ask questions and discuss the story as it unfolds, making connections with their own experiences and knowledge about digital safety and media literacy.

After the story is complete, facilitate a group discussion on the key themes and takeaways from the story. Ask questions like:

- What were the main digital safety issues presented in the story?
- How could the main character have prevented or mitigated the incident?
- What resources or strategies are available for improving digital safety and media literacy?

Conclude the activity by asking participants to develop a personal action plan for enhancing their digital safety and media literacy. This could include steps like updating passwords, setting up two-factor authentication, or attending a digital literacy workshop.

[Additional resources: https://avatarmaker.com/](https://avatarmaker.com/) Free online tool that can help you create an avatar. Consider using other AI tools to generate imagery based off the identity and narrative that the students develop. For example, [Microsoft Image generator](#) (free with a Microsoft account).

[If time permits... explore additional scenarios.](#)

Each group is provided with a scenario related to online behavior. In each, they should brainstorm and write down:

- What are the risks involved?

- What are the potential consequences of the action depicted in each scenario?
- What actions could lead to positive outcomes?

Groups can then share their top-level thoughts.

Scenario I – Are you in this video?

While eating lunch at work, Josef was looking through his Instagram newsfeed. Suddenly, his friend sent him a message. She asked, “Are you in this video?” with a link below it. Intrigued and excited, Josef clicked on the link, which led him to a page that appeared exactly like the Instagram login screen. Josef typed in his email and password but he was redirected to some random sites. Confused, he just shrugged it off and went back to work.

A few moments later, Josef was locked out of his Instagram account. The friend later called him, panicking. “I did not send that message! My account has been hacked and they are now using it to scam people.” Josef had been phished by hackers who now had his credentials for accessing personal messages and posts as well as potential means of scamming his friends and family.

Luckily, Josef was able to use the ‘forgot password’ option to recover his account since the attacker couldn’t change his recovery options without having access to his phone.

Takeaways:

- Connect with your friend before clicking on any suspicious links to verify if it is really them
- Enable two-factor authentication for all online accounts
- If your account is compromised, try to use the ‘forgot password’ option to get a password reset link on your phone

Scenario II – Catfish

For more than three months, Ivana had been exchanging messages with someone she met online. They seemed ideal – they were interested in her life, attentive and kind. They eventually proposed a face-to-face meeting, but when they demanded payment for their travel expenses, Ivana decided to investigate. She suspected that this was all a scam and found that the person’s profile pictures belonged to someone else after doing a reverse image search. The person she had been speaking with hadn’t been honest about their identity and had used stolen photos. After reporting the profile to the platform administrators, Ivana severed all communication.

Lessons learned:

- Be cautious when forming online relationships, especially if money is involved
- Verify the identity of online contacts through video calls and other means
- Report suspicious profiles and activities to platform administrators

Scenario III – Keylogger

Stefanie worked on an important group project for her chemistry class. One afternoon, she decided to use one of the school library computers to log into her email account and download some documents for the project. However, Stefanie didn't realize that the computer had been infected with a keylogger – a malicious piece of software designed to capture keystrokes and send them to a remote attacker. As she typed in her email address and password, the keylogger recorded every keystroke and transmitted her credentials to the hacker. That evening, Stefanie attempted to log into her email from her home computer but received a message that her password had been changed. She had been locked out. The attacker, using the stolen credentials, had not only accessed her email but also her social media and other linked accounts, causing chaos and compromising sensitive personal information.

Takeaways:

- Whenever possible, use your own trusted devices to access important accounts. Avoid logging into personal accounts on public or shared computers
- Enable two-factor authentication on all accounts where possible
- Avoid using the same password across multiple sites
- Be aware of signs of malware and ensure public computers are regularly scanned and maintained for security threats
- Use incognito or private browsing mode that automatically forgets your browsing history and logins as soon as you close the window. While this may not protect you against keyloggers, it usually will safeguard you against people who might take advantage of a logged-in account

Wrap-up (5 mins)

Ask students to reflect on one thing they learned about digital identity and how they can apply it in their own online activities.

MINI LESSON: HOW TO CREATE “UNCRACKABLE” PASSWORDS (1 HOUR)

The objective of this mini lesson is to educate participants about creating strong, uncrackable passwords using passphrases and to introduce the concept of [two-factor authentication \(2FA\)](#) as an additional layer of security.

Core concepts: Understanding password security principles and developing skills to create unique, safe and uncrackable passwords that are easy to remember.

An uncrackable password is resistant to unauthorized access attempts and almost impossible to decipher or guess. It does not follow predictable patterns – it is long and unique, does not contain common words or phrases, and does not contain personal information.

Password security principles are guidelines for creating, managing and using passwords to ensure protection against unauthorized access. They include: complexity (mix of uppercase and lowercase letters, numbers, special characters), length, uniqueness (one password per account), and multi-factor authentication (e.g. one-time codes).

Learning objectives:

- Understand password security principles
- Know what makes an uncrackable password and why it's important
- Be able to create their own uncrackable password

Warm-up (5 mins)

Start by revisiting the user-generated story that participants created. Highlight key elements of the story, especially the digital safety issue faced by the main character. Use the story's context to segue into the importance of creating strong passwords and using additional security measures. Highlight common issues like password reuse and easy-to-guess passwords. Have an informal discussion with students about the ways in which they use social media – what apps they use, how they use them, if they feel safe, if they have ever had their accounts hacked (what happened, if they recovered their accounts), etc.

Have you ever heard about *uncrackable passwords*? What do you think they are?

Engage (10 mins)

Students are invited to write down the most uncrackable password they can think of. They fold the paper and place it in an envelope. This will serve as a baseline for their current understanding of password strength. Then, in groups, they look at all the passwords and rank them in order from the most uncrackable to the most crackable one.

Explore (5 mins)

Students work in groups and focus on one of the passwords. They come up with ideas on how to improve it.

Explain (5 mins)

What do you think an uncrackable password's characteristics are? How could you create an uncrackable password which is safe, unique and easy to remember?

Explain the concept of passphrases. A passphrase is a sequence of words or a sentence that is easy to remember but hard to crack. Unlike single-word passwords, passphrases provide better security due to their length and complexity. For instance: IOnceMetAFamousMovieStar!

Students are invited to create their own passphrase. They should think of a memorable sentence or a combination of words that are easy for them to remember but difficult for others to guess. Encourage them to add complexity by including numbers, punctuation, capital letters, and symbols similar to letters (e.g., MyDogLoves-2PI@y!). Provide a few minutes for participants to come up with their passphrase and write it down on a separate piece of paper.

Elaborate (15 mins)

Once everyone has their passphrases, ask them to compare their original password with the new passphrase. Discuss the differences in complexity and security. Highlight how much more secure and memorable the passphrases are compared to traditional passwords. Students discuss what makes their new password uncrackable, taking into account the password security principles.

Transition into a discussion about additional security measures. Explain that even with a strong password or passphrase, accounts can still be vulnerable. Introduce the concept of two-factor authentication. Explain how 2FA adds an extra layer of security by requiring not just a password but also a second piece of information, like a code sent to their phone or generated by an authentication app.

Wrap-up (5 mins)

Students discuss about what they learned during this mini lesson.

- What is an uncrackable password?
- Why is it easy to remember?
- What are the password security principles?
- What is 2FA?
- What challenges do they foresee in implementing stronger passwords and

2FA in their daily digital habits?

- Encourage participants to share any personal experiences related to the benefits of digital security

Conclude the activity by encouraging participants to take immediate steps to enhance their digital security:

- 1 Update weak passwords to stronger passphrases.
- 2 Enable two-factor authentication on their important accounts.
- 3 Use a password manager to securely store and manage passwords.

Additional Resources:

- Books on digital security from the American Space
- Google Safety Center (<https://safety.google/>) – Security Checkup
- Kaspersky – How to create a strong password (<https://support.kaspersky.com/common/windows/3730>)
- How secure is my password (<https://howsecureismypassword.net/>)
- Microsoft Password Checker (<https://www.microsoft.com/ro-ro/security/>)

MINI LESSON: DIGITAL FOOTPRINT (90 MINS)

The objective of this mini lesson is to deepen participants' understanding of their digital footprint – that is, the trail of data they leave behind online (including social media posts, online purchases, and search history) and its implications for privacy, security, and their personal and professional reputation. This mini lesson will allow participants to learn proactive strategies to safeguard their digital identities and exercise appropriate caution.

What is a digital footprint?

Talk to the person next to you about the concept and try to come up with a definition, which could include:

- Whenever you use the internet, you leave behind a trail of information known as your digital footprint. A digital footprint can grow in many ways:
 - posting on social media
 - subscribing to a newsletter
 - leaving an online review
 - shopping online
 - websites can track your activity by installing cookies on your device, and apps can collect your data without you knowing it

Why does your digital footprint matter?

- Discuss in small groups
- Report back to the class

Elaborate by discussing the impact of pictures posted online.

- 1 Friend requests from hacked profile: Public pictures can contribute to a larger footprint. Discuss how hackers might use publicly available information to impersonate or target individuals.
- 2 Job application: Discuss how employers consider digital footprints during the hiring process. Public pictures can influence perceptions and impact professional opportunities. Colleges and universities can check their prospective students' digital footprints before accepting them too.
- 3 Discussion of privacy settings: Relate this to managing digital footprints by discussing how privacy settings on social media platforms can control what others see.

Some other ideas to touch on:

- Digital footprints are relatively permanent and once the data is public – or even semi-public, as may be the case with Facebook posts – the owner has little control over how others will use it
- A digital footprint can determine a person's digital reputation, which is now considered as important as their real-world reputation
- Words and photos which you post online can be misinterpreted or altered, causing unintentional offense

Investigating someone's digital footprint

Divide participants into small groups. Choose a classmate from a different group and investigate their digital footprint and try to come up with a few conclusions about what they like, what their interests are, what they are like. Make a profile. Share your findings with the person you profiled. Then, if they are comfortable with it, share it with the whole class.

Stop for reflection: Is there anything you regret sharing online? What could you do to clear your digital footprint of that material? Write down your ideas on post-it notes and stick them on the flipchart. Discuss these ideas as a whole class – how universal are they? How did this make you feel?

Active vs. Passive digital footprints

Classify the following into active or passive:

- Social media posts
- Browsing history
- Cookies
- E-mails
- Comments

- Online subscriptions
- IP addresses

Discuss these scenarios in terms of their connection to each individual's digital footprint. What is potentially problematic?

- 1 Maria is 23. She posts a picture of herself and her friends at the pool with a caption alluding to consumption of alcohol. She looks rather tipsy.
- 2 Joyce is 19. She likes to let her friends know where she is at all times. She checks in at a club on Friday night. This Friday, she just accepted a friend request from a good-looking young man.
- 3 Mario is 19. He wants to become a police officer once he finishes high school. He likes to post pictures of himself partying and stories and reels of him driving his new car at night while listening to loud music.
- 4 Tina is 17. She checks in for a vacation at a beautiful seaside resort where she has traveled with her parents. She posts a lot of pictures to let her friends enjoy the beauty of the places she is visiting.

Reflection:

Facilitate a group discussion on learnings from the activities and how participants can apply them to manage their digital footprints effectively. Encourage participants to create an action plan for reviewing and enhancing their privacy settings, updating passwords to passphrases, and monitoring their online presence regularly.

Additional activities:

- Celebrity hunt: Students are asked to look up examples of celebrities whose social media activity has destroyed their reputation. They then discuss how this might apply to them and whether they've ever had similar online activity.
- Digital detox challenge: Students take a digital detox for a period of 1–3 days, during which they do not use any digital tools (e.g., no Internet or mobile phones). They are asked to journal their experiences and feelings. Then they meet up to discuss their reflections and conclusions about their digital habits and the changes that they want to make.
- Privacy settings review: Students review their privacy settings on various platforms and draw conclusions about how safe their online presence is, and what changes they need to make.
- Digital footprint campaign: Students create posters, videos or any other awareness-raising material of their choice to address the problem of the risks of one's digital activities on their life. The campaign could target younger peers and could be posted/shared by the American Space.

MINI LESSON: BE A VILLAIN (45 MINS)

The objective of this activity is to raise awareness about the misuse of personal data, including selling, using and manipulating data for malicious purposes. Participants will explore the implications of data breaches and unauthorized access through interactive discussions. It encourages proactive thinking about safeguarding personal information and highlights the importance of cybersecurity measures in both personal and professional contexts. The mini lesson achieves these aims by putting the students in the shoes of a “villain” who has obtained personal data.

Learning objectives:

- 1 Understand the potential consequences of data breaches
- 2 Recognize the value of personal data
- 3 Develop a more cautious approach to sharing information online

Introduction (5 mins)

Introduce the activity by explaining that participants will role play as villains who have access to sensitive personal data. Emphasize that this is a hypothetical exercise to understand the consequences of data misuse. Briefly explain the concept of a data breach: unauthorized access to personal or sensitive information.

Role playing as a villain (15 mins)

Divide students into small groups. Ask groups to brainstorm and discuss what they would do if they had access to personal data (e.g., social media profiles, financial information, health records). Encourage them to think about potential motives such as identity theft, financial fraud or reputational damage. Here are some discussion topics:

- 1 **Sell the data:** Discuss the possibility of selling collected data on the dark web or to third-party entities. Highlight the underground economy of data sales and the potential financial gains for villains.
- 2 **Use the data:** Explore different ways villains might use the data for personal gain or malicious purposes. This could include accessing bank accounts, impersonating individuals, or conducting phishing attacks.
- 3 **Manipulate the data:** Focus on the manipulation of data to deceive or harm individuals or organizations. Discuss the reasons behind data manipulation, such as spreading misinformation, influencing public opinion or disrupting operations.

This group work could also be framed around discussing scenarios:

- You've gained access to a database containing names, email addresses, and phone numbers of 10,000 high school students in your city
- You've hacked into a popular fitness app and now have access to users' health data, including their daily step counts, heart rates, and GPS-tracked running routes
- You've obtained a list of credit card numbers and expiration dates from recent customers on an online shopping website
- You've accessed the email account of a local small business owner, which contains correspondence with clients and financial information
- You've acquired the login credentials for several social media accounts belonging to an up-and-coming social media influencer

Have each group share their ideas. Use the whiteboard/flipchart to:

- Write down key points from the group presentations
- Write down or create a visual diagram showing:
 - Data that can be breached (personal info, financial data, social media accounts)
 - Potential misuses of this data (identity theft, financial fraud, blackmail)
 - Consequences for victims (financial loss, reputation damage, emotional distress)

Class discussion (10 mins)

What if this happened to your data? Transition into a group discussion on the implications of data misuse if it were to happen to participants themselves. Facilitate a structured discussion to reflect on the insights gained. Encourage participants to share their thoughts on the potential impacts of data misuse and how they can apply this knowledge to protect their own data. Discuss practical steps individuals and organizations can take to enhance data privacy and security, such as using strong passwords, enabling two-factor authentication and being cautious with sharing personal information online.

How would students feel if their own data was compromised in these ways? What steps can they take to protect their personal information?

What types of personal data do you think are most valuable to cybercriminals? How could seemingly harmless information be used maliciously? What are some potential long-term consequences of having your data misused?

MODULE WRAP-UP: PERSONAL DIGITAL SAFETY PLEDGE (10 MINS)

The objective of this activity is to empower participants to commit to concrete actions that promote personal digital safety and data privacy after completing the workshop. This wrap-up activity not only reinforces the workshop's content but also encourages participants to take tangible steps towards enhancing their digital safety practices. It fosters a sense of community responsibility and empowers individuals to make informed decisions about their online presence.

- 1 **Reflection and discussion:** Begin by asking participants to reflect on the workshop's key takeaways regarding digital safety and data privacy. Prompt them to share one thing they found most valuable or surprising from the session.
- 2 **Personal pledge creation:** Distribute paper for participants to write down their personal digital safety pledge. Encourage them to consider specific actions they will take to enhance their online security based on what they learned.
- 3 **Sharing and commitment:** Invite participants to share their pledges with the group. This can be done in pairs or small groups, depending on the workshop size, to foster discussion and accountability.
- 4 **Group reflection:** Facilitate a brief discussion on the importance of personal accountability in maintaining digital safety. Ask participants to share any challenges they foresee in fulfilling their pledges and brainstorm strategies to overcome them.
- 5 **Closing remarks:** Conclude the workshop with closing remarks that emphasize the collective commitment to digital safety and data privacy. Highlight the impact of individual actions in creating a safer online environment for everyone.

MODULE

Understanding Social Media Algorithms

ALGORITHMS OVERVIEW

Social media algorithms are mathematical formulas used by social media platforms to determine the content that will be shown to each user. These algorithms take into account factors such as the user's past behavior, the popularity of the content, and the relevance of the content to the user's interests. The goal is to provide a personalized experience for each user, showing them content that is most likely to be of interest to them.

Social media algorithms have a significant impact on individuals and society as a whole. On the one hand, they can help users discover new and relevant content that aligns with their interests and values. This can lead to increased engagement, connection, and community-building among users. For example, an individual who is interested in fitness may see more content related to exercise and wellness, which can motivate them to adopt healthier habits.

However, social media algorithms can be harmful in a number of ways.

They can have negative impacts on mental health and well-being, as the more time people spend on social media, the more likely they are to experience negative emotions such as anxiety and depression. This is in part due to the constant stream of content, which can create feelings of comparison, inadequacy, and FOMO (fear of missing out). The algorithms can also contribute to this by showing users content that is designed to be addictive and to keep them engaged for as long as possible. This leads to more ad revenue for the social media companies, which are driven by profit, and not necessarily by the well-being and experience of their users.

Social media algorithms can also create echo chambers, where users are only shown content that aligns with their existing beliefs and interests, limiting exposure to diverse perspectives and leading to the spread of misinformation. Additionally, they can be manipulated by bad actors to spread propaganda, hate speech and other harmful content.

In terms of privacy, social media algorithms can also pose risks to individuals and groups. By tracking users' behavior and preferences, algorithms can create detailed profiles of users, which can be used for targeted advertising, political manipulation or other purposes. This can lead to concerns about surveillance, data mining and the potential for abuse. Furthermore, social media algorithms can amplify the harms of online harassment and cyberbullying, as they can prioritize content that is abusive, threatening or harmful. This can create a toxic online environment that is hostile to marginalized groups and individuals, and can have serious consequences for mental health and well-being.

It is important for users to be aware of these potential harms and to take steps to protect themselves, such as taking care of personal data, diversifying their social media feeds and limiting their time spent on these platforms.

Definitions

Digital footprint is the trail of data that individuals leave behind as they use digital devices, applications, and platforms, which can be actively or passively collected, stored, and analyzed by various entities.

Cookies and online trackers are technologies that collect user data, allowing websites to recognize users and deliver personalized content, while also enabling advertisers to target specific audiences.

Informed consent refers to the process of ensuring that users are fully aware of and agree to the terms and conditions, privacy policies, and potential uses of their data before they engage with a platform.

Forced consent is the requirement for users to agree to terms allowing big tech companies to collect and use their personal data in order to use a product or service, often without full understanding or meaningful choice.

Echo chamber (social media) is an environment where users are primarily exposed to information, opinions or beliefs that mirror their own.

Rabbit hole (social media) refers to a situation where users find themselves diving deeply into a specific topic, often driven by algorithms that suggest related content.

Liar's dividend is a phenomenon where the presence of misinformation and the ease of its spread enable individuals to deny the truth by calling it "fake news".

Surveillance economy is a business model where platforms collect, analyze and monetize users' data.

Attention economy refers to the concept that human attention is a scarce and valuable resource in the digital age, which can be commodified, bought and sold through various attention-seeking platforms and strategies.

Algorithmic black box refers to the secrecy of big tech companies surrounding the internal workings of their automated decision-making algorithms.

Data brokers are companies that collect, analyze and sell user data from various sources, including social media platforms. They compile detailed profiles on indi-

viduals and sell this information to advertisers, businesses and other entities for targeted marketing and other purposes.

Doomscrolling on social media is the act of continuously scrolling through negative or distressing news and posts, often leading to increased anxiety and stress.

Algorithmic fatigue on social media refers to the exhaustion and frustration users feel from constantly interacting with algorithmically curated content.

Overexposure on social media means sharing an excessive amount of personal information or content, leading to potential privacy risks, reputation damage and emotional or social consequences.

Learning Objectives

By the end of this module, participants will be able to:

- Define what social media algorithms are and how they work
- Explain what their impact is on individual and society
- Adapt their behavior online and build up resilience to algorithms

Learning Sequence with Activity Plan Steps

Warmer

Start by introducing yourself and ask participants to do the same.

Ask them which social media they use most often and how often, what they like about them or dislike, and do they have any concerns about their favorite platforms. By this time, they will probably mention Snapchat, Instagram, TikTok, maybe even Facebook. Ask them how much they pay for their social media activities (probably nothing or next to nothing). Does that mean that social media is free or cheap? If so, how did they become some of the world's richest and best-known companies, developing extremely sophisticated technology, collectively known as Big Tech (FANG(AM), Magnificent 7, etc.)?

Activity

Following two games should help participants realize the basic mechanics of social media algorithms:

Game 1 – Teenage Clicks

Draw a table. Put participants' names in column header and add 3 rows for each participant. If there are too many of them, this can be adjusted. Either pick 3–5 volunteers, or hand out pieces of paper to everyone, asking them to make a list. Once everyone has completed their list, these can be collected and consolidated into the table.

Ask participants which social media they use the most, and vote/pick the one they all use the most.

Ask them to do a quick scroll online and write down the first three ads they are shown. If someone does not feel comfortable about sharing some ad, they can skip it and go to the next one.

They will see that the same social network shows different ads in each of their feeds. Ask why that is and let them come up with their own ideas.

Game 2 – People vs Big Tech

Split the participants into two groups.

One group will be the said social network executives. They will need to come up with ideas regarding content they will serve to users, based on the data from the table, to keep them engaged and monetize their attention.

The other group will be users of that social network. They will need to come up with ideas on how to protect their privacy and avoid being overexposed. Maybe they can come up with things that should not be shared online, no matter what.

At this point, you should be able to understand their level of knowledge about the topic.

If there is enough knowledge and time to go deeper into how algorithms work and how different social media platforms are optimizing them, continue with **Mini Lesson 2 – Going deeper into the social media algorithms.**

If a less technical and more ‘human’ plan would work better, use **Mini Lesson 3 – Effects of algorithms on young people.**

MINI LESSON: GOING DEEPER INTO SOCIAL MEDIA ALGORITHMS

What are we talking about when we talk about algorithms?

Start by explaining the algorithm. The simplest way to define it is a set of step-by-step instructions designed to solve a certain problem. A dinner recipe or a home to school roadmap are simple algorithms we are “programmed” to execute daily. Ask: how does your phone find the number when you start to type your friend’s name in a phonebook? Basically, it eliminates the names you are not searching for. If it was you living in the landline telephone era, looking for a number in a 1000-page phonebook, how would you approach this task? If their idea is to “divide and conquer”, turning batches of pages at once instead of turning pages one by one, there they are using a search algorithm based on a recursion loop (the one that repeats the action of solving smaller instances of the same problem). You can mention a game where a person guesses the name on their forehead (<https://en.akinator.com/>) using an elimination logic as another example. However, search algorithms are just one algorithm type.

When we talk about algorithms driving social media and e-commerce sites, they are collectively called [recommender systems](#). Recommender systems are complex systems (as opposed to linear systems: think of road traffic vs. railway tracks) made of algorithms that analyze user behavior and various content characteristics to prioritize and tailor the information that appears in users’ feeds, home pages, etc. Here comes a rough division of social media algorithms:

Content processing (relatively fluid)	Content propagation (relatively stable)
Face recognition	Search
Image filters	Content recommendation (feeds)
Annotation (e.g. image tagging)	Ad delivery and targeting
Audio transcription	Content moderation
Language machine translation	Notification
Augmented and virtual reality	Trending
Friend recommendation	

While all these algorithms are important, we will focus on content propagation algorithms. **Content recommendation ones generate our social media feeds.** They

aren't limited to social media or user-generated content: movie recommendations on Netflix and product recommendations on Amazon belong to the same class of algorithms. Why focus on recommendation algorithms? Compared to search, recommendation drives a bigger (and increasing) fraction of engagement. More importantly, the platform has almost complete control over what to recommend a user, whereas search results are relatively tightly constrained by the search term. Even the "recommendation algorithm" on any large platform is in fact a whole suite of algorithms, but they are tightly coupled, so we refer to them collectively as "the algorithm". The primary objective of almost every recommendation algorithm on social media platforms is to rank the available content according to how likely it is that the user in question will engage with it, and engagement is a means to high-level goals: getting users to come back and drive ad revenue.

Social media companies have little incentive to be transparent about their recommender systems. Since their revenue comes from advertisement, clear rules would give way to "hacking" from marketers (business users). However, we know some universal rules.

A new user starts with a blank profile/feed and quickly adds input to the engagement prediction algorithm. Although an email address is usually enough to open an account, the information users reveal about themselves is potentially endless: birth date, age, gender, marital status, sexual orientation, schools, hobbies, what they like to eat, listen, watch, where they go and with whom. There are also innocent looking pastimes, quizzes and psychological tests (e.g. Which Disney character are you?) There is also a context that can be quite telling: geolocation, devices found in proximity and other data used for creation of shadow accounts. Content propagation moves from subscriptions (likes, follows...), network (friends, followers, connections...), and algorithm ("How did users similar to this user engage with posts similar to this post?"). In the meantime, their feed is filled with targeted ads, and it becomes what soap operas used to be for soap manufacturers.

There are three main types of signals that are available: network, behavior and demographics.

Network refers to the user's interaction with others: following, subscription, commenting, and so on.

Behavior is the most critical signal. Two users are similar if they have engaged with a similar set of posts. Its importance is a matter of sheer volume. Here's a simple calculation: If a user spends an hour a day on TikTok for four years, with the average video length of 20 seconds, and they skip half the videos, the platform has interaction records on over half a million videos for that single user.

Demographics refers to attributes such as age, gender, and, more importantly, language and geography. Demographic information is useful when a user first joins the platform since there is little else to rely on. But once the user starts leaving a behavioral record, its importance rapidly diminishes.

Let's have a look at some flavors:

Previous interaction / collaborative filtering	The mother of all signals, championed in recommendation systems of Amazon and Netflix. Amazon optimized their recommendation on previous purchases (“users who bought this also liked”), while Netflix suggested movies based on aggregated user ratings. In 2006, when many major social networks did not exist, and when those who did still had chronologically sorted feeds, the Netflix Prize was a \$1 million open competition for the best collaborative filtering algorithm to predict user ratings for films, based on previous ratings without any other information about the users or films.
Expected watch time	YouTube optimizes for it heavily, but Twitter/X does not as it is not video based.
Video watched to completion	TikTok algorithm amplifies and incentivizes very short videos under 15 seconds—which are more likely to be played to completion.
Content-based filtering	Udemy optimizes its course recommendations based on content metadata.
Content analysis	Spotify needs coherent playlists, rather than individually liked but unrelated song lists, so it optimizes more for content, and less for behavior. To make it up, they state reasons for their recommendations.
MSI	Meta (Facebook, Instagram) optimized for Meaningful Social Interactions, a weighted average of Likes, Reactions, Re-shares and Comments, before moving to machine learning models.

But, with so much material being published and floating around, and given the finite attention of the users, there can be only a certain amount of top performing content at any given time, and competition for popularity is intense. Most of the engagement comes from a small fraction of content that goes viral. Viral content

dominates attention, attention drives engagement, and engagement creates virality, closing the circle with more and more data being fed to the algorithms.

Here’s where things get tricky. These algorithms are not just sorting posts; they’re manipulating our emotions. Ever wondered why we see so many posts that make us angry, anxious or overly excited? That’s the algorithm at work. It knows that emotionally charged content is more likely to keep us engaged. And while we’re busy reacting to these posts, the platform is collecting data on our emotional triggers. In the 21st century, it is not an exaggeration to say that data has become the most valuable commodity, surpassing even the traditional treasures like oil or gold. Data can be exchanged, filed, archived, replicated, bought and sold. This is where data brokers come into play. The manipulation of public opinion over social media platforms has emerged as a critical threat to public life. Let’s have a look at the sales pitch of a Cambridge Analytica, the company that used data obtained from Facebook to achieve desired election outcomes for anyone who would hire them:

<https://www.youtube.com/watch?v=omc-5zj70MO>

Interaction type multipliers, Facebook

2017, Internal leaked memo (Meaningful Social Interactions formula, used after EdgeRank), Interaction type	Weight	2020, Facebook files (not clear if there have been further changes)	Weight
Like	1	Like	1
Reaction, Reshare without Text	5	Reaction	1.5
Non-sig comment, Non-sig reshare, Non-sig Message, Rsvp	15	Reshare	1.5
Significant Comment, Significant Reshare, Significant Message	30	Comment	15–20
Groups Multiplier (non friends)	0.5		
Strangers Multiplier (non-friend-of-friend)	0.3		

We can see how Facebook dropped the reshare multiplier after the March 2018 Cambridge Analytica scandal and separated comments from reshares. However, Facebook changed its algorithm since then and moved to machine learning, so we are in the dark when it comes to current multipliers. However, we can imagine that the principle of driving engagement is still at its core.

As we can see, we are the product. Our best way to build some resilience is to learn digital literacy best practices and try to protect ourselves from overexposure.

Additional Resources:

- <https://www.humanetech.com/the-social-dilemma>
- <https://www.thesocialdilemma.com/educators/>
- <https://www.humanetech.com/youth>
- <https://mediasmarts.ca/teacher-resources/foryou-algorithm-game>
- <https://firstdraftnews.org/long-form-article/understanding-information-disorder/>
- <https://doctorow.medium.com/my-mcluhan-lecture-on-enshittification-ea343342b9bc>
- https://dcrp.berkman.harvard.edu/tool/social-media-and-algorithms?utm_source=pocket_shared

Trivia:

- <https://jesperbalslev.dk/kranzbergs-six-laws-of-technology/>

MINI LESSON: EFFECTS OF ALGORITHMS ON YOUNG PEOPLE

MINI LESSON OBJECTIVES

At the end of the mini lesson, students will:

- know the negative side effects related to the use of social networks (comparison, anxiety, addiction, cyberbullying...)
- know what steps to take to reduce the negative impact of social networks
- evaluate current digital technology trends and their impact on society (limits and risks)

ENGAGE / STAR WARS

Let's ask students who likes Star Wars.

Imagine a situation where a classmate posts the following video on Instagram/TikTok.

<https://youtu.be/HPPj6vilBmU>

How would people react to it?

What negative/mocking reactions can your students imagine?

What can they imagine would happen if this video went viral?

EXPLORE / GRANDMA

Divide the class into 5 smaller groups and introduce the situation:

Your grandmother bought a smartphone and wants to start using social networking. She would like to be more informed about what's going on at home and in the world while expanding her horizons in the areas she enjoys in her spare time. She chose Facebook, Instagram, TikTok, YouTube and Telegram. The challenge is to answer questions that the grandmother has for all of the social networking sites:

Who do I follow?

What should I watch out for?

Am I in any danger?

How should I respond to posts?

Is it true that over time I can adjust the content I see to what I like to follow?

Each group chooses one social network and presents answers to the questions Grandma has in front of the others. At the end, we will write a simple guide for grandma on how to use it safely for specific social networks. In this activity, the students are in the role of those who can be a positive example for their family.

EXPLAIN

What

Social networks – risks:

- they don't represent reality at all (but usually only perfectly good moments)
- they force us to compare ourselves (in the negative sense that we are not good enough)
- likes trigger a dopamine rush in the brain
- pathological mobile checking (addiction and FOMO – fear of missing out)
- fake news: conspiracy theories, misinformation and hoaxes spread rapidly on social networks

How

Limit the negative impact of social networks:

- Cancel all notifications on mobile: (we really won't miss anything if we check all the news at once in an hour and not right now)
- Set limits on the apps we use: download an app that tracks how much time we spend on what app and alerts us when we exceed the limit
- Limiting Instagram when we don't feel right (we can, for example, have a call with a good friend instead)
- Regular offline activity (walk outside, run, meet up with friends)
- If someone is feeling very unwell, anxious, even depressed, it is a good idea to contact a professional. It does not have to be in person, there are anonymous online or telephone helplines

Why

- Young people who spent more than 3 hours a day on social networking sites are more likely to suffer from mental health problems than those who did not use social networking sites at all
- Dopamine from likes can cause states ranging from short-term joy to anxiety and contributes to addiction to social networking sites

ELABORATE

We will divide the students into 5 groups. Each group has to make a suggestion for a healthy online/offline regimen on different occasions. Their task is to describe the appropriate and inappropriate use of a smartphone on a given occasion and what we should be careful of:

- 1 at school
- 2 when learning
- 3 out with friends

- 4 when eating
- 5 when getting up and going to sleep

Students have 8 minutes to think about and write down their answers. If they run out of ideas, they can use their smartphones and search online when giving advice. They then briefly present their recommendations to the class.

EVALUATE

What new things have the students learned? They will be tested in a quiz. Use a quiz platform that you prefer.

1. Phenomena that have multiplied because of social networks

- a FOMO (✓)
- b cyberbullying (✓)
- c attention deficit disorder (✓)
- d digital detox

2. Social networks create bubbles because

- a we choose who we follow (✓)
- b it is easy to spread untruths
- c they do not represent reality
- d algorithms choose content for us based on our likes/hearts (✓)

3. What are the manifestations of mobile addiction?

- a nervousness when you leave your phone at home (✓)
- b nervousness when the phone is dead (✓)
- c nervousness when you don't have data/access to Wi-Fi (✓)
- d being on your mobile phone all the time (first thing when you get up, last thing before you go to bed) (✓)

4. What are the withdrawal symptoms of mobile phone addiction?

- a nervousness (✓)
- b mood swings (✓)
- c sleep problems (✓)
- d inattention (✓)

5. When you are studying, what helps you concentrate?

- a start with a review of events on Instagram
- b turn off all notifications (✓)
- c practicing gratitude
- d flight mode (✓)

MODULE

Online Behavior

USER GUIDE

The mini lessons provided in this module are intended to be constructed in the manner that best fits each instructor's interests and learning environment. Each mini lesson is approximately 15 to 20 minutes in length and can be utilized along or in conjunction with related lessons from this module. Included with these materials is a PowerPoint presentation that each instructor can modify to fit all or only selected mini lessons. The slide deck is organized to align to the topic flow outlined in the table of contents and this document. You may utilize all or only selected portions of this material that fit your needs.

At the end of this document you will find a compiled glossary, organized alphabetically by term, to support your instruction.

Enjoy!

MINI LESSON 1: HUMAN RIGHTS ONLINE

1 Theme/Module: Online Behavior

Subtopic: Human Rights on the Internet

2 Core Concepts/Overview of Topic

This part of the module will cover definitions and core concepts of human rights in general and human rights on the Internet.

3 Definitions (major concepts defined)

[Human rights](#) are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion or any other status. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more.

[Freedom of speech](#) is a principle that supports the freedom of an individual or a community to articulate their opinions and ideas without fear of retaliation, censorship, or legal sanction.

[Right to work](#) is the concept that people have a human right to work, or to engage in productive employment, and should not be prevented from doing so.

[Right to education](#) is a human right which recognizes a right to free primary education for all, an obligation to develop secondary education accessible to all, as well as an obligation to develop equitable access to higher education.

[Freedom of information](#) is freedom of a person or people to publish and consume information.

[Right to privacy](#) is a fundamental right and is considered essential to live a life of dignity and individuality.

- 4 Length of Mini Lesson (duration in minutes) (*Please note that each mini lesson should run 60–90 minutes; with the possibility of having multiple mini lessons)

20 mins

- 5 Description of Target Audience (number of people, age, level of knowledge) (*Please note that the basic target audience is 15–25 years of age)

High school students, 15–18

- 6 Learning Objectives (what the participants will be able to do by the end of each activity)
 - Objective 1:** Defining and providing core concepts of human rights related to the Internet
 - Objective 2:** Identifying different human rights
 - Objective 3:** Encouraging thinking about exercising human rights on the Internet
- 7 Materials, Supplies, and Technology (what’s needed to carry out the activities)
 - 1 Computers or phones with internet access and presentations
 - 2 Overhead projector or Smartboard
 - 3 Sticky notes and markers
- 8 Prep Work (for the workshop facilitator/teacher)

The teacher prepares learning materials in advance, researching about human rights and human rights on the internet. The teacher prepares sticky notes, presentations and chairs in a circle.
- 9 Mini Lesson Sequence with Activity Plan Steps (may typically include Warmer, Introduction to topic, Sequence of Activities, including ‘engage’, ‘explore’, ‘explain’, ‘elaborate’, ‘evaluate’ activities, and Wrap-Up)

Subtopic: Human Rights on the Internet

Warmer:

Slide 1: *Human Rights vs. Human Rights on the Internet*



Note:

For print purposes, photos in the Digital Literacy Toolkit can be replaced with others of a similar theme.

Brainstorming: Teacher asks students:

- 1 What can you infer from the photo?
- 2 What does this photo remind you of?
- 3 What is the first thing that comes to mind when you hear the words: human rights/human rights on the Internet?
- 4 Can you think of some concepts of rights?

Students come up with ideas.

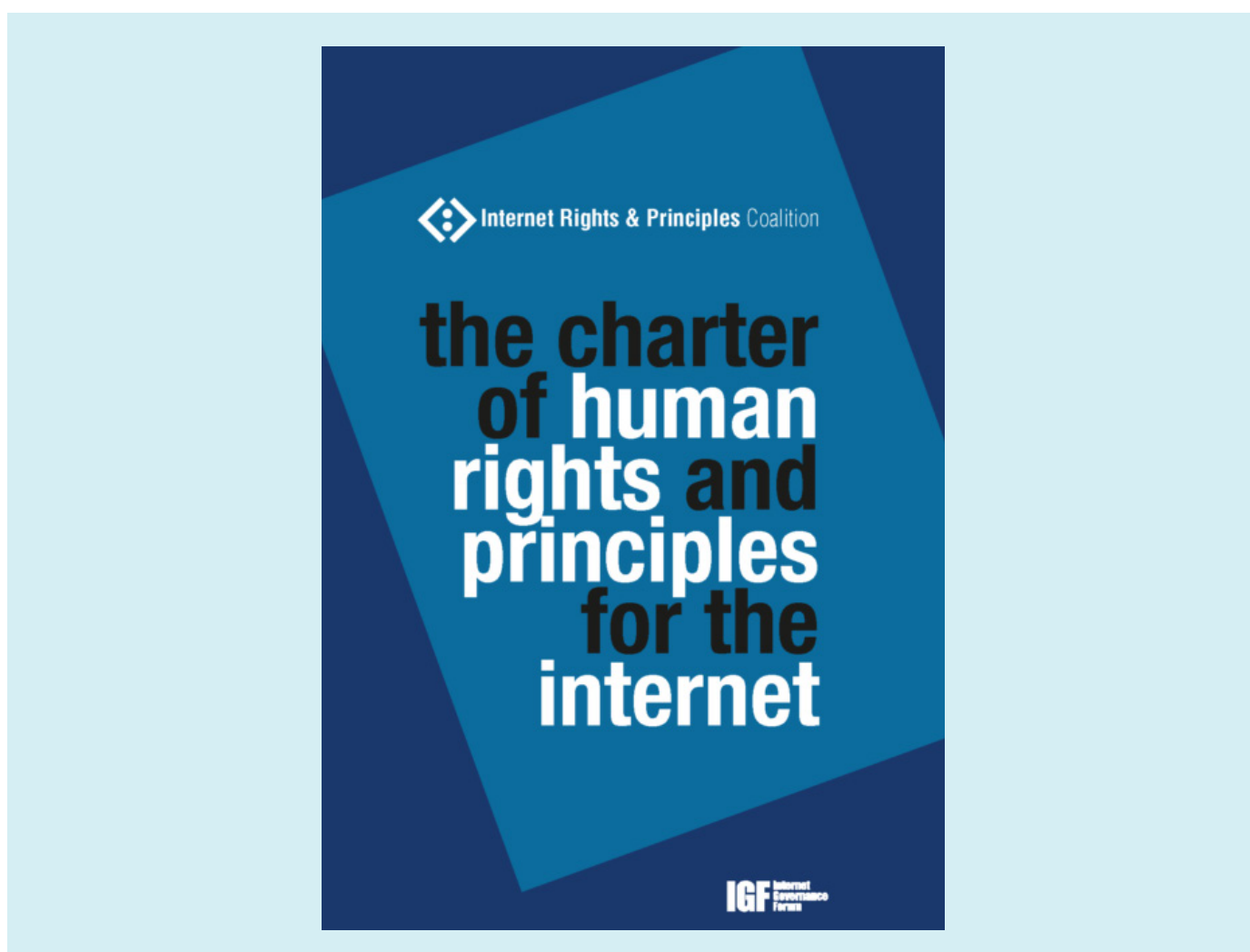
- After brainstorming, the teacher gives short “definitions” of rights according to the UN.

Slide 2:

“Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more.”

- Teacher states that there are only human rights in general, not human rights on the internet, officially declared, which does not mean that there are no rights on the internet and refers to the Charter of Human Rights and Principles for the Internet composed by IRP Coalition Governance supported by the UN:

Slide 3:



<https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf>

- Teacher advises the students to go through the Charter and learn more about their rights on the Internet.

Presentation (Main part): Activity – Who am I?

Slide 4: Basic Human Rights Related to the Internet



- Teacher asks the students to think about and mention some of the basic human rights and which ones are related to the Internet.
- Teacher presents 5 photos for 5 rights.

Activity: Who am I?

- Students are asked to sit in a circle and one of them is in the middle with a sticky note on the back with the name of one of the rights. The other students give him/her definitions, examples and hints to guess which right is written on his/her back.
- 5 students take turns for 5 rights.

Slide 5:

Basic rights related to the Internet:

- 1 Freedom of speech
- 2 Right to work
- 3 Right to education
- 4 Right to information
- 5 Right to privacy

- In this activity students were encouraged to think of the basic human rights and how they are related to the Internet on their own.

Wrap-up: 2 mins

Theory vs. the experience

Technique: **It made me think...**

- Teacher asks students to reflect on the presentation of the rights and think of one word or very short phrase that captures their opinion and completes the phrase “_____, it made me think.” The phrase can describe the experience they had related to the rights on the internet. After they’ve had a moment to think, students go around the circle and say their word or words, followed by the phrase “It made me think.” They can have more than one example.

Slide: “..., it made me think.”

Example:

- I tried to access a university site to get more info for my project paper, but had to pay to get more info, it made me think.
- I tried to express my disagreement on a political situation, but the administrator blocked me, it made me think

10 Discussion Questions (list of questions to discuss the topic/theme covered; may be used at different stages of the mini lesson)

Introduction questions:

- What can you infer from the photo?
- What does this photo remind you of?
- What is the first thing that comes to mind when you hear the words: human rights/human rights on the Internet?
- Can you think of some concepts of rights?

- 11 Suggested Follow-Up (possible variations of learning activities, tailored to older or younger audience than targeted specifically in the mini lesson)

Links:

- https://egov.ufsc.br/portal/sites/default/files/human_rights_and_the_internet_a_review_of.pdf
- <https://www.rand.org/pubs/commentary/2021/09/the-implications-for-human-rights-in-the-digital-age.html>
- <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf>
- <https://www.un.org/en/academic-impact/harnessing-power-internet-support-human-rights>
- <https://www.youtube.com/watch?v=JN8vXFUv8sA>
- <https://www.youtube.com/watch?v=EkBr3oZSQFY>

MINI LESSON: ONLINE VIOLENCE/HATE SPEECH

- 1 Theme/Module: Online Behavior
Subtopic: Hate Speech

- 2 Core Concepts/Overview of Topic

Despite all of the beneficial aspects that the Internet has provided in the modern era, it is frequently used as a forum to spread hatred and violence against specific individuals, groups of people and communities. This program will cover topics such as what hate speech is in the digital space, what laws limit it, how it affects the online spaces in which it occurs, and how young people can respond to it.

- 3 Definitions (major concepts defined)

Hate speech is any form of expression through which speakers intend to vilify, humiliate, or incite hatred against a group or a class of persons on the basis of race, religion, skin color, sexual identity, gender identity, ethnicity, disability, or national origin. Source: ala.org

Freedom of speech is the right to speak, write, and share ideas and opinions without facing punishment from the government. Source: Cornell Law School

Online hate is posting and sharing hateful and prejudiced content against an individual, group or community. It can take the form of derogatory, demonizing and dehumanizing statements, threats, identity-based insults, pejorative terms and slurs.

Digital citizenship is the responsible and ethical use of technology to engage in a virtual or digital environment.

Digital space refers to what is displayed on the screen of a digital device (e.g. laptops, computers, tablets, or smartphones).

Cancel culture is a way of behaving in a society or group, especially on social media, in which it is common to completely reject and stop supporting someone because they have said or done something that offends you.

Social media Terms and Conditions or User Agreement refers to a legal document that outlines the rules, guidelines, and conditions users must agree to abide by when using a particular social media platform.

“We must confront bigotry by working to tackle the hate that spreads like wildfire across the internet.” ANTONIO GUTERRES, United Nations Secretary-General, 2023

- 4 Length of Mini Lesson (duration in minutes) (*Please note that each mini lesson should run 60–90 minutes; with the possibility of having multiple mini lessons)

2 x 45-minute mini lessons

- 5 Description of Target Audience (number of people, age, level of knowledge) (*Please note that the basic target audience is 15–25 years of age)

High School students, 16–19

- 6 Learning Objectives (what the participants will be able to do by the end of each activity)
 - Students will learn about scenarios where youth can be exposed to hate online.
 - Students will learn how to respond to hate speech in online space and social media platforms.
 - Students will discover how to recognize and report hate speech online
 - Students will gain digital and media literacy skills to identify and oppose hateful content online.

By the end of this 90-minute workshop, students will be able to:

- 1 Define hate speech and identify examples of hate speech online.
 - 2 Understand the impact of hate speech on individuals and communities.
 - 3 Develop strategies to combat hate speech and promote online literacy and digital citizenship.
- 7 Materials, Supplies, and Technology (what’s needed to carry out the activities)
 - 1 Computers or tablets with internet access
 - 2 Whiteboard and markers
 - 3 Handouts with examples of hate speech (optional)
 - 4 Pen and paper for each student

8 Prep Work (for the workshop facilitator/teacher)

Use the provided slides about hate speech as a guide for the mini lessons.

9 Mini Lesson Sequence with Activity Plan Steps (may typically include Warmer, Introduction to topic, Sequence of Activities including 'engage', 'explore', 'explain', 'elaborate', 'evaluate' activities, and Wrap-up)

Introduction and Warmer (10 mins):

- 1 Welcome the students and explain the purpose of the mini lesson.
- 2 Start with a brief discussion about what hate speech is and how it manifests on the internet.
- 3 Ask students if they have encountered hate speech online and share their experiences briefly.

Activity 2: Defining Hate Speech (20 mins)

- 1 Define hate speech: Speech that offends, threatens, or insults individuals or groups based on race, color, religion, national origin, sexual orientation, disability or other traits.
- 2 Show examples of hate speech found online ([Spinning Wheel Activity](#) (students given sentences to analyze examples of hate speech))
- 3 Discuss the impact of hate speech on individuals and communities, both online and offline.
- 4 Encourage students to share their thoughts and feelings about hate speech.

Activity 3: Analyzing and Evaluating (20 mins)

- 1 Divide the class into small groups.
- 2 Each group finds examples of online content (articles, social media posts, comments, etc.) containing hate speech.
- 3 Switch examples and instruct each group to analyze the content and identify the elements of hate speech present.
- 4 Have each group present their findings to the class, discussing the language used, the targeted group and the potential consequences.

Activity 4: Combating hate speech (20 mins)

- 1 Brainstorm strategies to combat hate speech and promote online literacy.
- 2 Discuss the importance of being critical consumers of online content and verifying information before sharing.
- 3 Introduce the concept of digital citizenship and responsible online behavior.
- 4 Role-play scenarios where students encounter hate speech online and practice responding appropriately.

Conclusion (10 mins)

- 1 Summarize the key points discussed during the mini lesson.
- 2 Emphasize the importance of empathy, respect, and understanding in online interactions.
- 3 Assign a reflection activity: Ask students to write a short paragraph about one thing they learned from the mini lesson and how they can apply it in their online activities. Add it to a Google doc and discuss.
- 4 Thank the students for their participation and encourage them to continue promoting positive online communities.

Homework Assignment Options:

- 1 Create a guide on how to respond to hate speech online.
 - 2 Research and find examples of positive online communities or initiatives aimed at combating hate speech, as well as guidelines.
 - 3 Write a short essay reflecting on the impact of hate speech on society and the role of individuals in promoting online literacy and tolerance.
 - 4 Interview family members about how hate speech has changed.
- 10 Discussion Questions (list of questions to discuss the topic/theme covered; may be used at different stages of the mini lesson)
- What kind of hateful behavior is prohibited under social media guidelines?
 - What are the penalties/sanctions for those who violate the rules?
 - What can social media consumers do if they detect hateful content? What are the best techniques for dealing with it?
 - Watch videos/discuss stereotypes and discrimination shown in videos
- 11 Suggested Follow-Up (possible variations of learning activities, tailored to older or younger audience than targeted specifically in the mini lesson)

12 Additional resources

- <https://futurefreespeech.org/hate-speech-case-database/>
- https://en.wikipedia.org/wiki/Hate_speech_laws_by_country
- <https://www.linkedin.com/pulse/freedom-speech-versus-hate-cancel-culture-conundrum-jasmine-lovell>
- https://www.wimbledoncollege.org.uk/_site/data/files/safeguarding/parent-guides/7CC371A7937DA2B64AD9DB3558EF4FE8.pdf
- <https://www.mminstitute.org/wp-content/uploads/2022/04/Analysis-of-narratives-containing-hate-speech-and-disinformation-1.pdf>
- https://www.mminstitute.org/wp-content/uploads/2023/06/uvrede-i-mrznja_III-dio.pdf
- [Boys and Girls on Stereotypes](#)
- [Prejudice](#)
- [“Different” short movie](#)

Note: Ensure that you create a supportive and inclusive environment throughout the mini lesson. Be prepared to address any sensitive topics or concerns that may arise during discussions.

MINI LESSON: CYBERBULLYING

1 Theme/Module: Online Behavior
Subtopic: Cyberbullying

2 Core Concepts/Overview of Topic

This mini lesson will cover strategies related to discerning different types of cyberbullying, as well as delve deeper into the implications of cyberbullying on students' mental, social and emotional wellbeing.

3 Definitions (major concepts defined)

Cyberbullying is a type of bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, texts, apps, or online in social media, forums, or gaming where people can view, participate in or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior.

Cyberstalking is the act of monitoring, false accusations and threats, often accompanied by offline stalking behavior.

Exclusion is intentionally leaving someone out.

Harassment is the continuous and persistent pattern of sending hurtful or threatening online messages with the intention of causing harm to the recipient.

Outing/Doxing is the deliberate disclosure of sensitive or personal information about someone without their consent, aiming to embarrass or humiliate them.

Trolling is the deliberate act of upsetting others by posting inflammatory comments online.

Flaming is when a person posts insults and profanity about the target or directly sending them hurtful messages.

Fake profiles are fake social media accounts set up with the intention of damaging a person or brand's reputation.

4 Length of Mini Lesson (duration in minutes) (*Please note that each mini lesson should run 60–90 minutes; with the possibility of having multiple mini lessons)

60 mins

- 5 Description of Target Audience (number of people, age, level of knowledge)
(*Please note that the basic target audience is 15–25 years of age)

High school students, 15–18

- 6 Learning Objectives (what the participants will be able to do by the end of each activity)
Objective 1: Defining and differentiating between different types of cyberbullying
Objective 2: Identifying types of cyberbullying
Objective 3: Raising awareness about the impact different types of cyberbullying have on students' mental, emotional and social wellbeing
- 7 Materials, Supplies, and Technology (what's needed to carry out the activities)
 1. Computers or phones with internet access and presentations
 2. Flipchart paper
 3. Matching cards with terms and definitions of different types of cyberbullying
 4. Handouts with situational descriptions of (four) different types of cyberbullying and discussion questions for groupwork
- 8 Prep Work (for the workshop facilitator/teacher)
The teacher prepares learning materials in advance
- 9 Mini Lesson Sequence with Activity Plan Steps (may typically include Warmer, Introduction to topic, Sequence of Activities, including 'engage', 'explore', 'explain', 'elaborate', 'evaluate' activities, and Wrap-up)

Introduction – Brainstorming (students contribute to an online questionnaire via Slido (<https://app.sli.do/event/vLNmfThQ44t2FBN7CzeFT9> / joining code: #1994794). Or, the instructor may use an online questionnaire app of their choice to conduct this activity.

- What is cyberbullying?
- Examples of cyberbullying
- What are the effects of cyberbullying?

Discussion

Match a type of cyberbullying with its definition

Students get a card either with a key word or with a definition of a key word. They walk around in an attempt to match each key word with its definition.

Matched pairs also demonstrated online: Matching pairs exercise
This exercise could be done online in small groups, individually or in person (terms and definitions are written on paper, one group of students has papers with terms, the other group has definitions, task is to find correct pairs).

Analyzing situations of cyberbullying in small groups

Questions: What type of cyberbullying is described in this situation? What would you do? Once students agree on the type of cyberbullying, they write down suggestions about what to do in each of the situations. The groups are given the chance to decide on their own how they would like to present their answers – whether through a step-by-step strategy they have come up with in their group, or by doing a roleplay demonstrating a solution to a specific problem involving a specific type of cyberbullying.

Situations:

- Jenny thought she could trust her friends, so she shared some personal secrets in a private group chat. However, one of her so-called friends, Lisa, took screenshots of their conversation without Jenny’s knowledge. Angry after a minor argument, Lisa decided to post these screenshots on social media, revealing Jenny’s secrets to everyone at school (outing).
- Jordan received a string of hateful messages on social media from an anonymous user. The messages insulted Jordan’s appearance and mocked a recent post by Jordan about a personal achievement. Despite blocking the user, this continued from new accounts created by the same person (harassment).
- Have you ever had someone constantly commenting on your social media posts, sending you unwanted messages, and showing up uninvited to your online conversations? This type of behavior can make you feel uncomfortable and intruded upon, similar to how you might feel if someone followed you around in real life, always watching and never giving you space. For example, imagine a situation where a classmate continuously sends you private messages on various platforms asking personal questions even after you’ve made it clear you’re not interested in talking to them. In a scenario like this, it’s important to recognize that your boundaries are being crossed and take steps to protect your online privacy (cyberstalking).

Dialogue Example:

Student A: “Hey, did you see those messages I’ve been getting from Jake lately?” Student B: “Yeah, it seems like he’s really not getting the hint that you’re not interested in talking to him. That’s not cool at all.”

- In the digital world, a wolf in sheep’s clothing is not just a tale but a stark reality. Imagine scrolling through your favorite social media platform and

stumbling upon a seemingly friendly account of someone claiming to share your interests. Let's say this account engages you in conversation, asking personal questions and building a sense of trust. However, little do you know, the person behind the screen is not who they claim to be. This deceptive individual might even go as far as spreading false rumors about you to tarnish your reputation, all while hiding behind the guise of a fabricated persona. In this scenario, Alex, a high school senior, finds a new Instagram friend who persuades Alex to share personal information. The conversation takes a turn as the mysterious "friend" begins to use this information to threaten Alex. This unsettling encounter exposes the danger of undisclosed identities online, showcasing how easily cyberbullies can exploit trust and anonymity to harm others (fake profile).

10 Discussion Questions (list of questions to discuss the topic/theme covered; may be used at different stages of the mini lesson)

Introduction questions:

- What is cyberbullying?
- Examples of cyberbullying
- What are the effects of cyberbullying?

Analyzing situations of cyberbullying in small groups:

- What type of cyberbullying is described in this situation?
- What would you do?

11 Suggested Follow-Up (possible variations of learning activities, tailored to older or younger audience than targeted specifically in the mini lesson)

- **Activity 1:** Instead of Slido, you can use another interactive digital tool of your choice, or you can do it without ICT application by offering to divide students in groups and have them write on flipcharts.
- **Activity 2:** This activity can either be done with matching pairs of cards and have students move around the room, or with the digital tool LearningApp, or you can combine both.
- **Activity 3:** The situations describing different types of cyberbullying should be adapted according to your students' age and language acquisition level.
- **Follow-up activity:** Advocates for Raising Awareness Against Cyberbullying (Have your students create a video/poster/reel/illustration with their own message related to fighting cyberbullying. This could be compiled in either a digital form of your choice or posted in the American Space as a class poster dedicated to the topic).

12 Additional resources

- <https://www.unicef.org/northmacedonia/cyberbullying-what-it-and-how-stop-it>
- https://www.youtube.com/watch?v=Jwu_7lqWh8Y
- <https://www.youtube.com/watch?v=TtEGAcLBTTA>
- https://www.analyticamk.org/images/2024/Cyber/_WEB_Anglisna_Verzija_-.pdf

NOTE: Ensure that you create a supportive and inclusive environment throughout the mini lesson. Be prepared to address any sensitive topics or concerns that may arise during discussions.

MINI LESSON: CANCEL CULTURE

1 Theme/Module: Online Behavior
Subtopic: Cancel Culture

2 Core Concepts/Overview of Topic

Cancel culture has gained significant visibility in recent years due to the rise of social media platforms that provide a public space both for controversies and for activism in support of accountability and responsible digital citizenship

3 Definitions (major concepts defined)

Cancel culture is a way of behaving in a society or group, especially on social media, in which it is common to completely reject and stop supporting someone because they have said or done something that offends.

Censorship is the action of preventing part or the whole of a book, film, work of art, document, or other kind of communication from being seen or made available to the public, because it is considered to be offensive or harmful, or because it contains information that someone wishes to keep secret, often for political reasons.

Free Speech is the right to express your opinions publicly.

Political correctness is the act of avoiding language and actions that could be offensive to others, especially those relating to sex, gender and race.

Accountability is the fact of being responsible for what you do and able to give a satisfactory reason for it, or the degree to which this happens.

(source: Cambridge Dictionary)

4 Length of Mini Lesson (duration in minutes) (*Please note that each mini lesson should run 60–90 minutes; with the possibility to have multiple mini lessons)

5 Description of Target Audience (number of people, age, level of knowledge) (*Please note that the basic target audience is 15–25 years of age)

Group of 20, 15–18 (or 18–25)

- 6 Learning Objectives (what the participants will be able to do by the end of each activity)
 - understand the concept of cancel culture
 - discern credible information from sensationalized content by evaluating online evidence
 - analyze different perspectives on cancel culture, considering both its potential benefits and drawbacks
 - reflect on the long-term consequences of cancel culture on society (diversity of opinion, mental health, accountability, etc.)

- 7 Materials, Supplies, and Technology (what's needed to carry out the activities)

Internet connection, laptop, overhead projector.

- 8 Prep Work (for the workshop facilitator/teacher)
 - Familiarize yourself with core concepts and context of the example
 - Practice lateral reading
 - Create a slideshow/presentation with examples and main ideas (optional)

- 9 Mini Lesson Sequence with Activity Plan Steps (may typically include Warmer, Introduction to topic, Sequence of Activities, including 'engage', 'explore', 'explain', 'elaborate', 'evaluate' activities, and Wrap-up)

- Warmer – vocabulary work, brainstorming
What are some other common attributes of human beings? Create a concept map/word clouds
- Engage – Is there anything wrong with this?/What is wrong with this tweet? (J.K. Rowling tweet) – Elicitation
- Explore – Research on the topic, in 4 groups, on different aspects of the situation:
Potential tasks to research:
 - Who is involved?
 - What is the target group of this message?
 - How was this message conveyed? (Techniques)
 - Who and how did others react to the message?
 - Is the message problematic? Why?/Why not?
 - Can you identify a local similar situation? How was that reflected in the media? What were the reactions to it?

- Explain – What is cancel culture? – Watch a video on YouTube for further explanation – <https://www.youtube.com/watch?v=STHIYh5HIVM>
 - What is cancel culture?
 - How does cancel culture manifest itself in the online public sphere through social media platforms?
 - Is cancel culture a concept you adhere to? Why?/Why not?
 - Are you aware of any other examples, closer to your community?
 - What are the potential benefits and drawbacks of cancel culture?
 - How do you avoid being “canceled”?
- Elaborate
Come up with alternative tweets to express ideas on the topic of cancel culture (use <https://zeob.com/> to generate tweets to use in the activity). What is cancel culture for you?
- Evaluate – Reflection
How easy was it for you to express your views using tweets? What did you find out? What did you learn? How do you feel?

10 Discussion Questions (list of questions to discuss the topic/theme covered; may be used at different stages of the mini lesson)

- 1 What is cancel culture?
- 2 How does cancel culture manifest itself in the online public sphere through social media platforms?
- 3 Is cancel culture a concept you adhere to? Why?/Why not?
- 4 Are you aware of any other examples, closer to your community?
- 5 What are the potential benefits and drawbacks of cancel culture?
- 6 How do you avoid being “canceled”?

11 Suggested Follow-Up (possible variations of learning activities, tailored to older or younger audience than targeted specifically in the mini lesson)

Further reading activity, for older audiences (18–25) <https://harpers.org/a-letter-on-justice-and-open-debate/> could generate for/against activities (speaking, writing) starting from the text.

Topics for debate:

Is cancel culture a product of academia or popular culture?

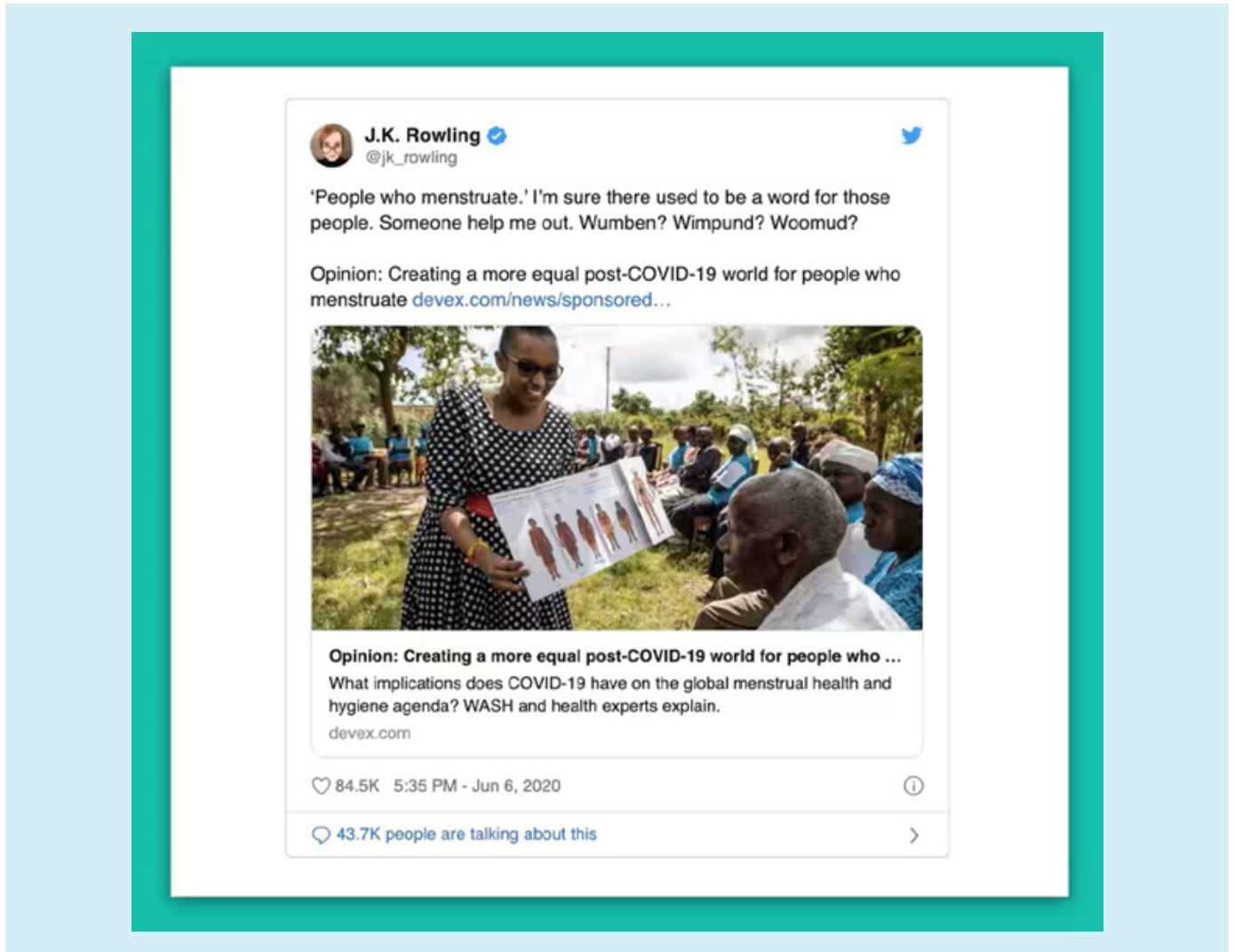
What are some solutions to the growing impact of cancel culture?

Should language change/adapt to convey new realities of the 21st century culture?

12 Additional resources

NOTE: The mini lesson should include all materials used, including presentations, handouts, and resources.

ORIGINAL TWEET



GROUP 1 – TWEETS AND CLIPPINGS OF NEWSPAPER ARTICLES THAT INCRIMINATE J.K. ROWLING

JK Rowling reignites row with Harry Potter stars Daniel Radcliffe and Emma Watson

11 April 2024

By Helen Bushby & Ian Youngs, BBC News

Share

BBC

Home News Sport Business Innovation Culture Travel Earth Video Live



Potter stars Daniel Radcliffe, Emma Watson and Rupert Grint attended a premiere in 2010

Radcliffe, who played the young wizard in the Harry Potter films, responded to Rowling's original posts in 2020 by saying: "It's clear that we need to do more to support transgender and nonbinary people, not invalidate their identities."

He added that he hoped the author's comments would not "taint" the movie series for fans.

Watson said: "Trans people are who they say they are and deserve to live their lives without being constantly questioned or told they aren't who they say they are."

Eddie Redmayne, star of *Fantastic Beasts* and *Where to Find Them*, based on Rowling's book, also said in 2020: "I disagree with Jo's comments. Trans women are women, trans men are men and non-binary identities are valid."

Meanwhile Rupert Grint said: "I firmly stand with the trans community... Trans women are women. Trans men are men. We should all be entitled to live with love and without judgment."

Ralph Fiennes, who played Potter villain Lord Voldemort, came to the author's defence, calling the abuse she received "disgusting" and "appalling".

Other stars including Eddie Izzard and Helena Bonham Carter, who played Bellatrix Lestrange, have also said they do not consider Rowling's views to be transphobic, but reflective of her own experience of abuse.

Rowling said she spoke out about transgender issues in part due to her personal experience of domestic abuse and sexual assault.



Chad "Don't Trust Deray" Vigorous @PrettyBadLefty · 8h

Replying to @jk_rowling

Honestly, it's amazing that you want this to taint your legacy. That this is something you want people to read on your in a biography about you or on your Wikipedia in 60 years.

30

88

6K



Chad "Don't Trust Deray" Vigorous @PrettyBadLefty · 8h

I just can't imagine what it must be like knowing that children in 50 years, or even less time, will read/ fall in love with your books only to find out what kind of person wrote them and be so disappointed but just not care

38

59

3.7K



1 more reply

© Twitter



h @halsey



Imagine writing a generation defining series about a youth uprisal that defeats a tyrannical monster motivated by the preservation of "pure blood" and looking at THIS time in the world and going "hmm...yep. I'm gonna invalidate trans people."

201K 9:09 PM - Jun 6, 2020



42.9K people are talking about this



Jonathan Van Ness @jvn · 12h
 Trans women are women. Trans Black people & trans non-Black people are discriminated against every single day. They're dying. We're fighting for Black people & trans people and you're doing this?

J.K. Rowling @jk_rowling · 16h
 If sex isn't real, there's no same-sex attraction. If sex isn't real, the lived reality of women globally is erased. I know and love trans people, but erasing the concept of sex removes the ability of many to meaningfully discuss their lives. It isn't hate to speak the truth.
[Show this thread](#)

217 7.2K 47.7K

[Show more replies](#)

Alexis @Alexis_Miller19 · 11h
 Replying to @jvn and @jk_rowling
 @jvn now is the time to also unfollow her, and encourage others to do the same.

1 11

Jonathan Van Ness @jvn · 1h
 Unfollowed and thought I already had 🇺🇸❤️

© Twitter / Jonathan Van Ness

BLM // ACAB @royallyqueer · 7h
 Replying to @jk_rowling
 That's interesting, because I have endometriosis and an IUD in place to treat it, and therefore, I no longer menstruate. I haven't had a menstrual cycle since early high school, and I'm 21. I guess I'm not a woman anymore? :/

124 67 4.7K

[5 more replies](#)

© Twitter

Mallory Rubin @MalloryRubin · [Follow](#)

Harry Potter is about the magic of love, acceptance, belonging. The power of courage. The impact of hope. Trying to take those things away from people is a terrible tragedy. Trans women are women. 🇺🇸❤️

2:57 AM · Jun 11, 2020

5K Reply Copy link

[Read 146 replies](#)

 **J.K. Rowling**  [@jk_rowling](#) · [Follow](#) 

Devastated and bewildered that my embrace of inclusive language has angered its most enthusiastic devotees, so let's just say:

Happy Mother's Day to all females who've raised children. 🌸❤️


 **J.K. Rowling**  [@jk_rowling](#)

❤️🌸 Happy Birthing Parent Day to all whose large gametes were fertilised resulting in small humans whose sex was assigned by doctors making mostly lucky guesses ❤️🌸

6:40 PM · Mar 10, 2024 


 77.3K  Reply  Copy link


[Read 2.2K replies](#)

<https://torontosun.com/entertainment/celebrity/happy-birthing-parent-day-j-k-rowling-ripp> 

TORONTO SUN

This advertisement has not loaded yet, but your article continues below.



 **Celebrity**




'HAPPY BIRTHING PARENT DAY:' J.K. Rowling ripped for Mother's Day post

The Harry Potter author, however, was unmoved by the reaction

Denette Willford
Published Mar 11, 2024 · Last updated Mar 11, 2024 · 2 minute read

 51 Comments 



British author J. K. Rowling attends HBO's "Finding The Way Home" world premiere at Hudson Yards on December 11, 2019 in New York City. PHOTO BY ANGELA WEISS/AFP/Getty Images

J.K. Rowling has sparked outrage once again on social media with a post marking Mother's Day in Britain.

The sarcastic comment came days after Rowling was reported to police over accusations of "misgendering" transgender news anchor India Willoughby.

Many commenters lambasted the best-selling author for her divisive post.

"Of all the ways Rowling could have used her star status to make a difference in the world, she chose to pick on a miniscule per cent of an already very demonized group of people," broadcaster Narinder Kaur replied. "So sad."

Ian Timbrell, a trainer on LGBT inclusion, wrote, "It breaks my heart to see how she is descending into trolling and unnecessary attacks."

Rowling, however, was unmoved by the reaction and wrote in a follow-up post: "Devastated and bewildered that my embrace of inclusive language has angered its most enthusiastic devotees, so let's just say: Happy Mother's Day to all females who've raised children."

GROUP 2 – TWEETS AND CLIPPINGS OF NEWSPAPER ARTICLES THAT SUPPORT J.K ROWLING

<https://www.theguardian.com/books/2022/dec/12/jk-rowling-launches-support-cent>

JK Rowling

● This article is more than 1 year old

JK Rowling launches support centre for female victims of sexual violence

Beira's Place will add to Edinburgh's existing rape crisis centre, which is run by a trans woman

Severin Carrell Scotland editor

Mon 12 Dec 2022 17:21 CET

Share



📷 The board of directors of Beira's Place (from left): Susan Smith, JK Rowling, Johann Lamont, Margaret McCartney and Rhona Hotchkiss. Beira's Place in Edinburgh will support women in the Lothians aged 16 and over who have experienced sexual violence or abuse at any time in their lives. Photograph: Nicole Jones/PA

JK Rowling is funding a new support and counselling service for survivors of sexual violence in Edinburgh.

The author, who has written about her own experience as a survivor of sexual assault, is setting up the new centre, called Beira's Place, because she believes there is an "unmet need for women" in the Lothians area.

The new project, which will be managed by two experienced specialists in rape crisis support, Isabelle Kerr and Susan Domminney, comes after a row about the role of transgender women in rape crisis services in [Scotland](#).

In line with a longstanding policy of trans inclusion by the country's official network, [Edinburgh](#) rape crisis centre has been run by a trans woman, Mridul Wadhwa, since May 2021.

Rowling said: "As a survivor of sexual assault myself, I know how important it is that survivors have the option of women-centred and women-delivered care at such a vulnerable time."

Critics of Scotland's [gender recognition changes](#), which culminate next week in a final vote by MSPs on a bill to introduce new self-declaration rules for trans people, believe that appointment dissuaded some female survivors of male sexual violence from using Edinburgh's centre.

Rowling has become a figurehead for gender critical feminists, who argue the changes erode hard-won protections for women.

Kerr said sexual offences "are gendered crimes that are overwhelmingly perpetrated by men and disproportionately experienced by women".

Hogwarts Legacy, a video game based on the franchise, seemingly introduces a trans character.

Per *Entertainment Weekly*, the hotly anticipated Hogwarts Legacy, a video game set in the *Harry Potter* universe, introduces a new character, Sirona Ryan, who is seemingly trans. Though Sirona, a barkeep at Three Broomsticks, is not explicitly labeled as transgender, a line of her dialogue is highly suggestive. Referring to her friendship with a goblin, she says, “Hadn’t seen him in years when he came in a few months ago. But he recognized me instantly. Which is more than I can say for some of my own classmates. Took them a second to realize I was actually a witch, not a wizard.”



Warner Bros. Games has already faced criticism over Hogwarts Legacy, which creates a new revenue stream for Rowling. When asked about the concerns by IGN, game director Alan Tew said, “We know our fans fell in love with the Wizarding World, and we believe they fell in love with it for the right reasons. We know that’s a diverse audience. For us, it’s making sure that the audience, who always dreamed of having this game, had the opportunity to feel welcomed back. That they have a home here and that it’s a good place to tell their story.”

<https://www.glamour.com/story/a-complete-breakdown-of-the-jk-rowling-trans-gender-comments-controversy>



Maya Forstater

@MForstater

I share the concerns of [@fairplaywomen](#) that radically expanding the legal definition of 'women' so that it can include both males and females makes it a meaningless concept, and will undermine women's rights & protections for vulnerable women & girls.



Екатерина

@koterigan



I signed up for Twitter just to say that I support J. K. Rowling. I deeply respect her for speaking out the truth and defending her position. And you're wishing her death for protecting women, really? Misogyny again, how classic. [#IStandWithJKRowling](#)
[#SolidarityWithJKRowling](#)

♥ 805 2:11 PM - Jun 7, 2020



💬 121 people are talking about this





The Telegraph

@Telegraph



JK Rowling should not be arrested for her views on transgender issues because the new Scottish hate crime law is a “terrible piece of legislation”, the Education Secretary has said.

Read more here

telegraph.co.uk/news/2024/04/0...

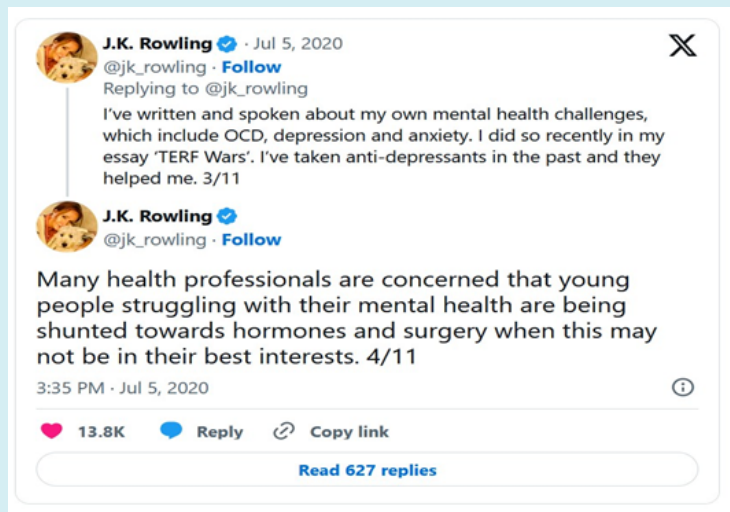


JK Rowling should not be arrested for trans views, says Gillian Keegan

11:14 AM · Apr 2, 2024 · 14.1K Views

40 Reposts 4 Quotes 147 Likes 4 Bookmarks





Helena Bonham Carter came to her defense.

Bonham Carter, who played Bellatrix Lestrange in the Harry Potter films, defended Rowling in a November 2022 interview with *The Sunday Times Magazine*.

"It's horrendous, a load of bollocks," she said of the Rowling backlash. "I think she has been hounded. It's been taken to the extreme, the judgmentalism of people. She's allowed her opinion, particularly if she's suffered abuse," Bonham Carter continued. "Everybody carries their own history of trauma and forms their opinions from that trauma, and you have to respect where people come from and their pain. You don't all have to agree on everything—that would be insane and boring. She's not meaning it aggressively, she's just saying something out of her own experience."

<https://www.glamour.com/story/a-complete-breakdown-of-the-jk-rowling-trans-gender-comments-controversy>

MINI LESSON: DEEPPFAKE TECHNOLOGY

- 1 Theme/Module: Online Behavior
Subtopic: Deepfake Technology
- 2 Core Concepts/Overview of Topic
Understanding deepfakes is crucial in today's digital landscape where misinformation and manipulation abound. As these sophisticated AI-generated videos blur the lines between reality and fiction, their potential to deceive and manipulate poses significant risks to various aspects of society, including politics, journalism, and personal relationships. By learning about deepfakes, individuals can better discern between genuine content and manipulated media, enabling them to safeguard themselves against misinformation, protect their privacy, and uphold the integrity of information dissemination in the digital age.
- 3 Definitions (major concepts defined)
Deepfake is a video of a person in which their face or body has been digitally altered so that they appear to be someone else.
Synthetic media is a catch-all term for the artificial production, manipulation, and modification of data and media by automated means, especially through the use of artificial intelligence algorithms.
- 4 Length of Mini Lesson (duration in minutes) (*Please note that each mini lesson should run 60–90 minutes; with the possibility to have multiple mini lessons)

15–20 mins

- 5 Description of Target Audience (number of people, age, level of knowledge)
(*Please note that the basic target audience is 15–25 years of age)

High school students, 15–18

- 6 Learning Objectives (what the participants will be able to do by the end of each activity)
 - Learn what deepfake technology is
 - Learn about potential uses and abuses of the technology
 - Learn what to pay attention to when dealing with online content that is suspected to be synthetic media
- 7 Materials, Supplies, and Technology (what's needed to carry out the activities)

Computer, projector, speakers

8 Prep Work (for the workshop facilitator/teacher)

Watch and read the provided materials about deepfake technology. Get familiar with the terminology and the different ethical dilemmas surrounding the use of the technology

9 Mini Lesson Sequence with Activity Plan Steps (may typically include Warmer, Introduction to topic, Sequence of Activities including 'engage', 'explore', 'explain', 'elaborate', 'evaluate' activities, and Wrap-up)

- Instructor introduces the topic of deepfake technology and asks students if they are familiar with it
- Students watch videos (embedded in the slide deck) of deepfake examples and discuss what they saw
- Discussion about the ethical implications of this technology for individuals and for society
- How to recognize deepfakes – students discuss and the instructor introduces a list of currently available resources on recognizing deepfake videos

10 Discussion Questions (list of questions to discuss the topic/theme covered; may be used at different stages of the mini lesson)

- Have you seen deepfake videos before?
- In what context?
- How confident are you that you would be able to tell that a video was generated by artificial intelligence?
- What implications do you think this technology might have on society?
- What implications do you think it might have on you personally?
- What are some of the uses you can think for this technology? Can you think of positive and negative ways in which this technology might be used?

11 Suggested Follow-Up (possible variations of learning activities, tailored to older or younger audience than targeted specifically in the mini lesson)

The suggested mini lesson can be expanded beyond the original 15-minute format by sharing more of the additional resources with the students, such as the educational website, showing how deepfakes are made and the video resource on the way deepfakes can affect democratic processes, both of which can serve as starting points for further discussion.

12 Additional resources

Deepfake overview

<https://www.discoverdatascience.org/articles/everything-you-need-to-know-about-how-to-use-deepfake/>

Deep Future (Tactical Tech)

<https://youtu.be/LarVQRTnGo0>

How deepfakes may shape the future

<https://theglassroom.org/en/misinformation-edition/exhibits/how-deep-fake-may-shape-the-future>

The making of a deepfake (Deepfake Lab)

<https://deepfakelab.theglassroom.org/>

Positive Application of Deepfake Technology

<https://www.dataart.com/blog/positive-applications-for-deepfake-technology-by-max-kalmykov>

Seeing Is No Longer Believing

<https://www.thomsonreuters.com/en-us/posts/technology/practice-innovations-deepfakes>

Twelve things we can do now to prepare for deepfakes

<https://lab.witness.org/projects/synthetic-media-and-deep-fakes/>

Deepfake Spotter Lab

<https://cdn.ttc.io/s/theglassroom.org/world-bank-group/red-deep-fake-spotter-English.pdf>

Are deepfake videos a threat to democracy (Lesson plan, Common Sense Media)

<https://www.commonsense.org/education/digital-citizenship/lesson/are-deepfake-videos-a-threat-to-democracy>

APPENDIX: GLOSSARY

Accountability is the fact of being responsible for what you do and able to give a satisfactory reason for it, or the degree to which this happens.

Cancel culture is a way of behaving in a society or group, especially on social media, in which it is common to completely reject and stop supporting someone because they have said or done something that offends.

Censorship is the action of preventing part or the whole of a book, film, work of art, document, or other kind of communication from being seen or made available to the public, because it is considered to be offensive or harmful, or because it contains information that someone wishes to keep secret, often for political reasons.

Cyberstalking is the act of monitoring, false accusations, and threats, often accompanied by offline stalking behaviors.

Deepfake technology is a synthesized digital media file that convincingly reproduces a person's likeness. Deepfakes can be utilized for both entertainment purposes as well as by bad actors for unsavory purposes.

Denigration is when a cyberbully denigrates a victim by sending, posting, or publishing false information online about the individual.

Digital citizenship is the responsible and ethical use of technology to engage in a virtual or digital environment.

Digital space refers to what is displayed on the screen of a digital device (e.g. laptops, computers, tablets, or smartphones).

Exclusion is intentionally leaving someone out.

Fake profiles are fake social media accounts set up with the intention of damaging a person or brand's reputation.

Flaming is when a person posts insults and profanity about the target or directly sending them hurtful messages.

Freedom of information is freedom of a person or people to publish and consume information.

Freedom of speech is the right to speak, write, and share ideas and opinions without facing punishment from the government. Source: Cornell Law School

Harassment is the continuous and persistent pattern of sending hurtful or threatening online messages with the intention of causing harm to the recipient.

Hate speech is any form of expression through which speakers intend to vilify, humiliate, or incite hatred against a group or a class of persons on the basis of race, religion, skin color, sexual identity, gender identity, ethnicity, disability, or national origin. Source: ala.org

Human rights are rights that belong to every person. For example, the right to life, the right to freedom from torture and cruel and inhumane treatment, freedom of religion, freedom of speech, and the right to health, education, and a reasonable standard of living.

Impersonation is when a cyberbully impersonates a victim by posting comments on social media and chat rooms in the individual's name.

Online hate is posting and sharing hateful and prejudiced content against an individual, group or community. It can take the form of derogatory, demonizing and dehumanizing statements, threats, identity-based insults, pejorative terms and slurs.

Outing/Doxing is the deliberate disclosure of sensitive or personal information about someone without their consent, aiming to embarrass or humiliate them.

Political correctness is the act of avoiding language and actions that could be offensive to others, especially those relating to sex, gender, and race.

Right to education has been recognized as a human right which recognizes a right to free primary education for all, an obligation to develop secondary education accessible to all, as well as an obligation to develop equitable access to higher education.

Right to privacy is a fundamental right and is considered essential to live a life of dignity and individuality.

Right to work is the concept that people have a human right to work, or to engage in productive employment, and should not be prevented from doing so.

Social media Terms and Conditions or User Agreement refers to a legal document that outlines the rules, guidelines, and conditions users must agree to abide by when using a particular social media platform.

Trolling is the deliberate act of upsetting others by posting inflammatory comments online.



IMPRESSUM

Title of the Guidebook:

Digital Literacy Toolkit

Implemented by:

Propulsion

Milutina Milankovića 9ž

11000 Belgrade, Serbia

Financed by:

U.S. Embassy

Bul. kneza Aleksandra Karađorđevića

92, 11040 Belgrade, Serbia

Responsible for Content:

Vildana Drljević Boljanić

Executive Director, Propulsion

Editor:

Ivana Jovanović, Propulsion

Proofreading:

Dušan Sekulić

Linguistic sign-off:

Milica Stamenković

Design and Layout:

Ivo Matejin, Propulsion

Year of Publication:

2024

Place of Publication:

Belgrade, Serbia

Contact Information:

Phone: +381 11 3343 999

Email: we@propulsion.one

Disclaimer:

This toolkit was produced with the financial support of the U.S. Embassy. While the contents of this book have been created with the utmost care, we are not responsible for the content of external links.



American Spaces