DIGCITY

Co-funded by the European Union

GAME-BASED DIGITAL CITIZENSHIP

Guide on Digital Citizenship Skills

LogoPsyCom PENS digiQ YuzuPulse

This guide is a part of the **DigiCity project** resources.

Discover more on the project website: **https://projectdigicity.eu/**

Project leader

Omladinski savez udruženja 'OPENS' (Serbia)

Participating organisations

Digitalna Inteligencia (Slovakia)

YuzuPulse (France)

Logopsycom (Belgium)

Table of contents

I. INTRODUCTION

In today's interconnected world, the digital landscape is as much a part of our daily lives as the physical one. From social media platforms to educational resources, the Internet offers endless possibilities for connection, learning, and creativity. However, navigating this vast and dynamic space requires more than technical skills; it demands a set of values, behaviours, and knowledge collectively known as digital citizenship.

This guide is designed to equip young people with essential digital citizenship skills, empowering them to participate responsibly, ethically, and effectively in the digital world. It addresses key topics such as online privacy, responsible social media usage, misinformation and how to recognise it, and what are digital footprints. These are not just skills, but life lessons that will help young people thrive in an increasingly digital society.

Why Did We Make This Guide?

The Guide on Digital Citizenship Skills serves as the foundational pillar for achieving the objective of fostering informed and responsible digital citizens. It systematically outlines the critical aspects of digital citizenship that trainers and youth organisations must grasp. By offering a comprehensive overview of topics like online privacy, responsible social media usage, and discerning misinformation, this guide equips trainers and educators with the essential knowledge to guide young learners effectively.

Through practical tips and inclusive activities, this guide emphasises critical thinking, ethical behaviour, and responsible digital communication. It establishes a theoretical framework by defining key concepts and providing actionable strategies to integrate digital citizenship principles into educational practices.

Why Does Digital Citizenship Matter?

The Internet is a powerful tool, but it can also pose challenges. Young people often encounter issues such as cyberbullying, misinformation, privacy breaches, and the long-term implications of their online actions. Without proper guidance, these challenges can hinder their personal, academic, and professional growth.

This guide seeks to bridge that gap by providing practical tips and engaging activities that are accessible to all. By emphasising critical thinking, ethical behaviour, and responsible communication, the guide aims to help young learners make informed decisions and foster positive interactions in digital spaces.

Who Is This Guide For?

- **Young people**: To help them build confidence and competence in navigating the digital world safely and responsibly.
- **Educators and trainers**: To provide tools and strategies to support young people in developing strong digital citizenship skills.
- **Youth organisations**: To enhance their educational practices by integrating digital citizenship principles into their programmes.

What to Expect?

The guide is structured into clear, user-friendly chapters, each focusing on a critical aspect of digital citizenship:

- **Understanding Digital Citizenship**: An introduction to the principles and values that define responsible participation in the digital world.
- **Digital Competences - Baseline Skills**: An overview of essential skills required for effective and safe digital engagement.

- **Media Literacy:** Understanding, recognising, and managing misinformation; tools and strategies for identifying credible sources and avoiding the spread of false information.
- **Responsible Social Media Use:** Risks, benefits, and e-reputation; insights into navigating social media responsibly, balancing its advantages with its potential risks.
- **Understanding and Managing Your Digital Footprint**: Guidance on how online actions shape personal reputations and future opportunities; practical advice for protecting personal information and managing privacy settings.
- **Glossary**: A helpful reference section defining key terms and concepts related to digital citizenship.

Each chapter includes actionable tips, relatable examples, and inclusive activities to engage learners of diverse backgrounds. The guide is designed to be both educational and practical, ensuring that digital citizenship principles can be applied in real-world contexts.

What Do We Want to Achieve?

This guide is more than an educational tool; it is a commitment to fostering a generation of thoughtful, ethical, and responsible digital citizens. Together, we can create a safer, more inclusive digital environment where everyone has the opportunity to learn, grow, and connect.

Let's embark on this journey to digital citizenship and empower young learners to become leaders in the digital age.

II. UNDERSTANDING DIGITAL CITIZENSHIP

Digital citizenship refers to the responsible and appropriate use of technology by everyone who engages with digital environments. It encompasses various behaviours, skills, and knowledge, such as protecting personal information, engaging in respectful communication, and contributing positively to online communities, necessary for navigating the digital world safely and effectively.

The concept of digital citizenship is crucial in today's interconnected world, where digital interactions are a significant part of daily life. Digital citizenship can significantly influence your online behaviour in several ways. It encourages you to behave responsibly online through respectful communication. Online users are more likely to engage in polite and considerate interactions, reducing instances of cyberbullying and online harassment. It also allows ethical content sharing and creation as everyone becomes more aware of copyright laws and intellectual property rights.

By following the principles of digital citizenship, you become more safety-conscious about protecting your privacy and learn to manage your digital footprint and protect personal information, reducing the risk of identity theft and online exploitation. Digital citizens are better equipped to identify and avoid online scams, misinformation, and potentially harmful content.

On the other hand, digital citizenship education improves your overall digital literacy by developing skills such as critical thinking. You learn how to critically evaluate online information, which leads to more informed choices and opinions and easier decision-making.

Digital citizenship also promotes active participation in online communities. You are more likely to engage in positive online activism, contribute constructively to digital communities, and understand the impact of online actions. It fosters empathy and consideration for others in digital spaces.

The Rights and Duties of Digital Citizens

One of the fundamental rights of digital citizens is the protection of personal data. The General Data Protection Regulation (GDPR), implemented by the European Union in 2018, is a landmark regulation that aims to protect the privacy and personal data of individuals within the EU.

KEY ASPECTS OF THE GDPR INCLUDE:

Data protection
Ensuring that personal data is collected, processed, and stored securely.

Right to access
Allowing individuals to access their personal data and understand its use.

Consent
Clear and explicit consent from individuals is required before collecting their data.

Right to erasure
Providing individuals with the right to request the deletion of their personal data under certain conditions.

The GDPR sets high data protection and privacy standards, serving as a model for other regions and reinforcing the rights of digital citizens.

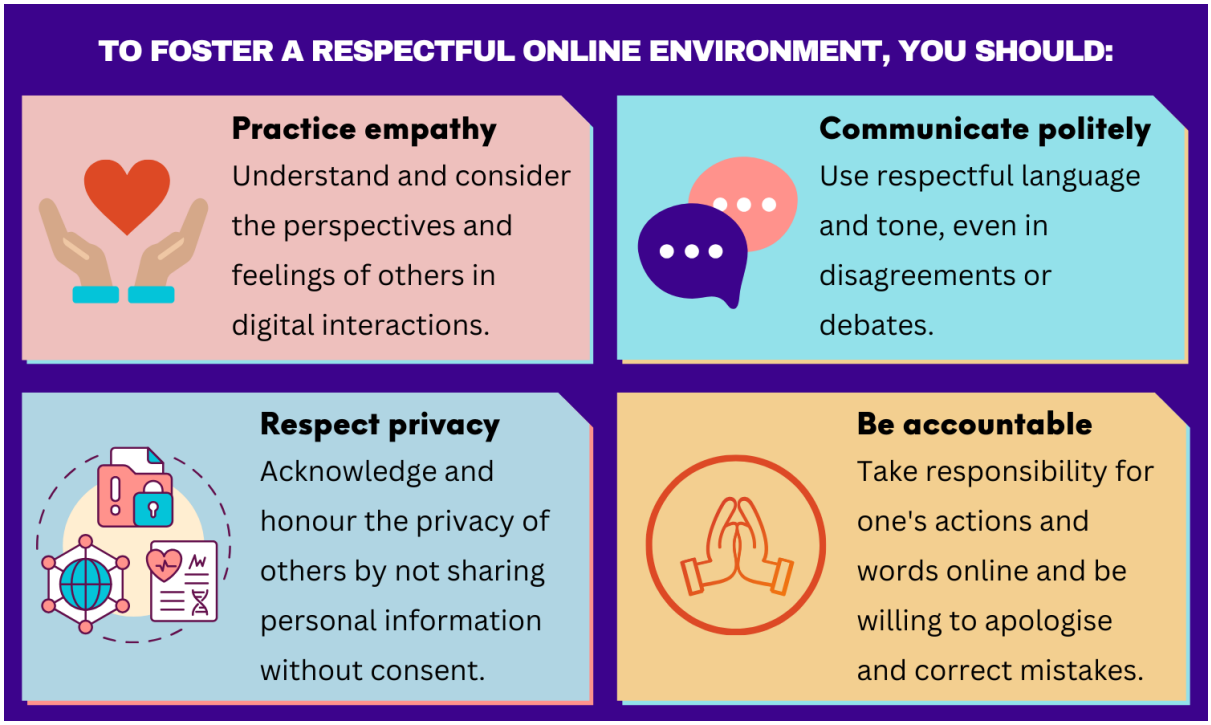
More information on **GDPR.eu page "What is GDPR, the EU's new data protection law?" (Wolford B, n.d.)**

There are several ways for you as a digital citizen to seek help and support when encountering issues online:

- **Online support communities:** Joining forums and groups where individuals share experiences and advice on dealing with digital challenges.
- **Helplines and hotlines:** Utilising dedicated helplines for issues like cyberbullying, online harassment, or digital addiction.
- **Reporting mechanisms:** Using reporting tools on social media platforms and websites to flag inappropriate or harmful content.
- **Educational resources:** Accessing online courses and tutorials to enhance digital literacy and understanding of digital rights.

Information about available resources empowers you to address and resolve online issues effectively. More information on **Find a Helpline**.

Respect is a cornerstone of digital citizenship.



By embodying these principles, you contribute to a positive and respectful digital community.

Digital citizens are also responsible for recognising and addressing discrimination and harmful behaviour online. This involves:

IDENTIFYING DISCRIMINATION

Be aware of biased or prejudiced content that targets individuals or groups based on race, gender, religion, or other characteristics.

EDUCATING OTHERS

Raise awareness about the impact of discrimination and promote inclusivity and diversity online.

REPORTING HARMFUL CONTENT

Use platform tools to report and remove harmful or abusive content.

SUPPORTING VICTIMS

Offer support and resources to individuals who have experienced online discrimination or harassment.

By actively opposing discrimination and harmful behaviour, you help create a safer and more equitable digital space for all users.

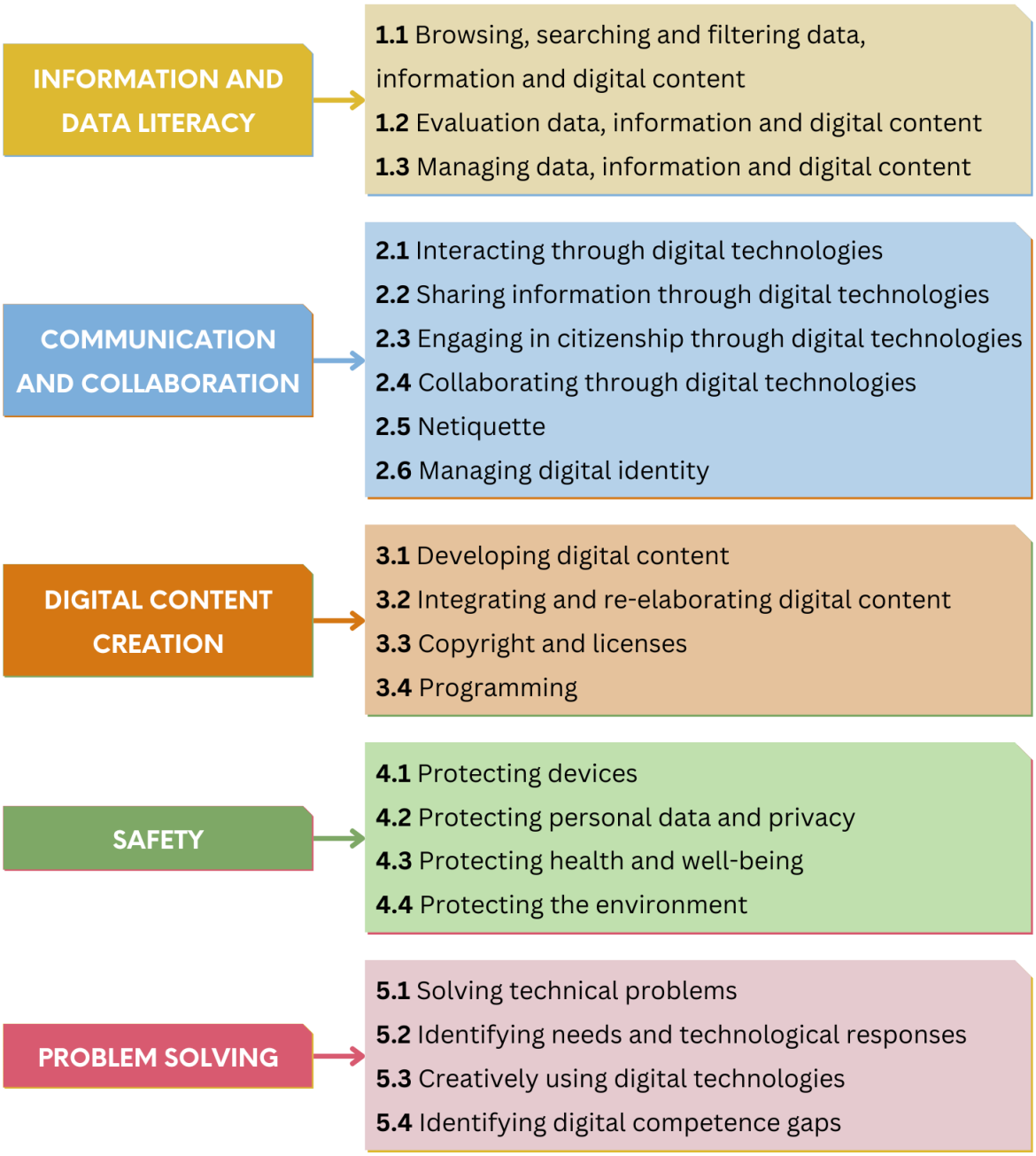
III. DIGITAL COMPETENCIES – BASELINE SKILLS

Definition of Digital Competencies

Defined by the European Commission's Digital Competence Framework for Citizens (**DigComp**), digital competencies are essential for engaging confidently, critically, and responsibly with digital technologies across various contexts, including education, employment, and personal life. They include a broad spectrum of skills, from basic computer literacy to advanced capabilities in digital problem-solving and ethical use of technology.

Frameworks like DigComp provide a structured approach to understanding the multifaceted nature of digital competencies. It emphasises the importance of accessibility, ensuring that digital competencies are inclusive and applicable to all citizens, regardless of their background or ability.

Source: Digital Competences Framework for Citizens (DigComp), European Commission



Information Literacy and Critical Thinking

Searching and Managing Information

Information literacy involves not just finding information but also assessing its quality and relevance. Techniques such as using advanced search operators, critically evaluating search results, and recognising credible sources are essential for navigating the vast amounts of data available

online. Tools like **Google Scholar**, academic databases, and reputable news outlets are examples of resources that you can use for reliable information.

Moreover, managing information extends to understanding how to store, retrieve, and protect data. This includes using digital tools for organising information, such as cloud storage solutions, and understanding data management principles, such as file naming conventions and data backup strategies. It also involves recognising the ethical implications of data use, such as respecting intellectual property and privacy rights.

Evaluating Sources

Misinformation and disinformation are prevalent online, which means you should develop the ability to assess the sources of information you encounter critically. This involves questioning the author's credentials, the accuracy of the information, and the presence of any potential biases. Lateral reading, fact-checking with multiple sources, and using tools like fact-checking websites (e.g., **Snopes**, **FactCheck.org**) are practical strategies that help you in this evaluation process.

Additionally, it is important to understand the impact of algorithms and personalised content delivery, which can skew the information presented to you based on your previous behaviours and preferences. Learning about the influence of algorithms on your information environment can empower you to seek out diverse perspectives and avoid echo chambers.

Problem Solving and Critical Evaluation

Problem-solving in digital contexts is more than technical troubleshooting; it requires a mindset of critical evaluation and adaptive thinking. Digital problem-solving skills include identifying digital needs, analysing potential solutions, and selecting the most effective strategies. For example, when facing an online security threat, such as phishing, you need to assess the situation, recognise the threat, and take appropriate actions like reporting the incident and enhancing your security measures.

Educational approaches that incorporate digital simulations, role-playing, and interactive problem-solving activities can help young people develop these competencies in engaging and practical ways. By providing real-world scenarios that require critical evaluation and decision-making, educators can better prepare their students for the complexities of the digital world.

Communication and Content Creation

Digital Communication Skills

Digital communication is a cornerstone of digital competence, including the skills needed to interact effectively in various online environments. Effective digital communicators are able to tailor their messages to their audience, choose the appropriate channels for communication, and maintain professionalism and respect in their digital engagements.

Acquiring digital communication skills includes exploring the concept of "netiquette" or guidelines for courteous and respectful behaviour online. It also involves discussions about digital footprints and the permanence of online actions, highlighting how important it is to think before posting and to understand the long-term impact of digital communication.

Online Collaboration Tools

Collaboration is a key component of modern work and learning environments, facilitated by digital tools that enable people to work together regardless of their physical location. Online collaboration tools, such as **Slack**, **Trello**, and **Asana**, offer platforms for teams to communicate, share files, and manage projects in real time. Mastering these tools is considered part of

digital competence, as they are widely used in both educational and professional settings to enhance productivity and foster teamwork.

These tools can be integrated into classroom activities to teach students about project management, communication, and collaboration in digital spaces. For example, group projects that require students to use digital collaboration tools can help them develop practical skills in managing tasks, communicate effectively, and work together towards a common goal.

Basics of Content Creation

Digital content creation involves producing various forms of digital media, such as text, images, videos, and interactive content. This competence is not limited to technical skills and it includes creativity, understanding audience needs, and applying ethical considerations, such as respecting copyright and avoiding plagiarism. Basic content creation skills include using digital tools for editing, designing, and publishing content, as well as understanding the principles of digital storytelling.

You should experiment with different content creation platforms, from blogging to video production, to build your skills and express your ideas. Understanding the basics of content creation also involves recognising the role of visual design and user experience, which are essential in making digital content engaging and accessible. Additionally, you should learn about the importance of accessibility in digital content, ensuring that your creations are inclusive and that diverse audiences can use them.

IV. MEDIA LITERACY

Definition and Scope

Media literacy empowers you to access, analyse, evaluate, create, and engage with media content across various platforms. It involves understanding the nature of media messages, the processes of media production, and the role media plays in shaping society. Media literacy also includes recognising the power dynamics in media ownership and the economic, political, and cultural influences that drive media content.

The scope of media literacy has expanded significantly in the digital age, encompassing traditional media like newspapers and television, as well as digital media such as social media, podcasts, blogs, and streaming services. As new technologies emerge, such as artificial intelligence and augmented reality, the scope of media literacy continues to evolve, requiring ongoing education and adaptation. This broader scope shows the need for a comprehensive approach that integrates media literacy education into various subjects and aspects of everyday life.

Understanding Media Messages

Understanding media messages requires the ability to critically analyse how media constructs reality. Media messages are not neutral; they reflect the intentions and biases of their creators, which can influence how you perceive and interpret the information. Media producers use various techniques, such as framing, selection of sources, visual imagery, and emotional appeals, to shape their messages and affect your perceptions.

For example, the use of dramatic visuals in news coverage can amplify the emotional impact of a story, potentially leading to heightened public concern or panic. Similarly, the omission of certain perspectives or voices can alter the understanding of an issue, presenting a one-sided view. By learning to deconstruct these messages, you can identify the underlying assumptions and biases, leading to a more nuanced understanding of media content.

Development of these analytical skills can be supported through activities that involve comparing different media portrayals of the same event, discussing the influence of media ownership on news coverage, and exploring how advertising strategies shape consumer behaviour.

Recognising and Managing Misinformation

Misinformation is a pervasive challenge in today's media landscape, where the speed and reach of digital communication can amplify false or misleading information. In order to recognise and manage the impact of misinformation, it is important you understand its different types:

- **Fabricated content:** Includes completely false information created to deceive. For example, a fake news article that falsely claims a celebrity has died can spread quickly on social media, causing confusion and distress.
- **Clickbait:** Refers to sensational or misleading headlines designed to attract clicks and drive traffic to websites, often at the expense of accuracy. For instance, a headline like "You Won't Believe What This Politician Did!" may lead to an article that exaggerates or distorts the facts to entice readers.
- **Deepfakes:** Manipulated videos or images that depict people saying or doing things they never did, created using artificial intelligence. An example could be a deepfake video of a public figure, such as a politician, making a statement they never actually made, which can be used to spread false narratives or discredit them.

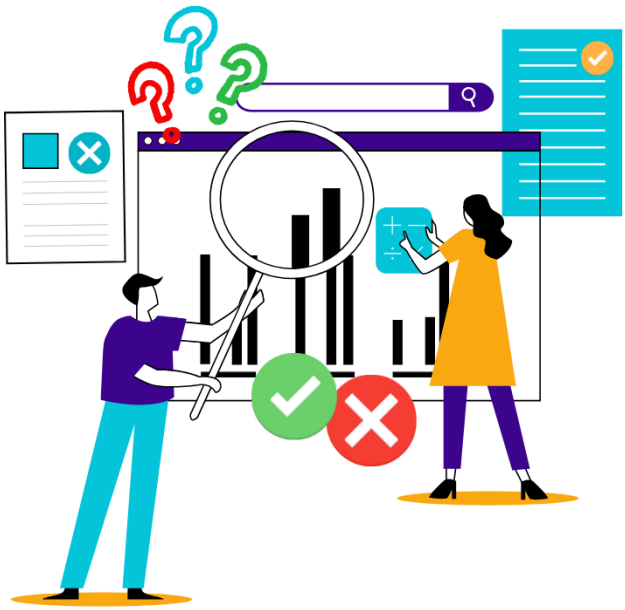
- **Misleading content:** Information that distorts reality or presents facts in a misleading way. For example, using a photo from an unrelated event to represent current news can trick viewers into thinking it's connected to the story being reported.
- **False context:** Genuine information presented in a misleading context, altering its intended meaning. An example is an old photograph from a past protest being used to represent a current event, giving viewers the impression that the situation is ongoing or larger than it is.
- **Impostor content:** Involves content that impersonates genuine sources. For example, fake websites mimic the appearance of reputable news outlets to spread false stories, making it difficult for readers to distinguish between real and fake news.
- **Satire or parody:** Satirical content, such as articles from websites like **The Onion**, intended to entertain, but that can be mistaken for factual reporting if the audience is unaware of its satirical nature.
- **False attribution:** Crediting a piece of content or a quote to a false or non-existent source. For example, attributing a fabricated quote to a well-known scientist or public figure to lend unwarranted credibility to a claim.
- **Rumours and hoaxes:** Unverified information that spreads through social networks, often creating false impressions or panic. A classic example is the viral spread of hoaxes about product recalls or false health advice, such as the myth that drinking hot water can prevent COVID-19.

Fact-Checking and Verification

Fact-checking and verification involve systematically evaluating the accuracy and reliability of information by consulting multiple sources, examining evidence, and using verification tools. Key steps in effective fact-checking are:

- **Source evaluation:** Start by checking the credibility of the source. Reputable sources typically have transparent editorial standards, provide author details, and disclose any potential conflicts of interest.

- **Cross-referencing:** Compare the information with other reputable sources. Consistency across multiple credible sources increases the likelihood that the information is accurate.
- **Using verification tools:** Tools like **Google Reverse Image Search** can help verify the authenticity of images, while browser extensions like **NewsGuard** provide ratings on the credibility of news websites.
- **Checking author expertise:** Evaluate whether the author is qualified to speak on the topic. Experts or recognised authorities in the field are more likely to provide reliable information.
- **Analysing evidence:** Look for supporting evidence, such as data, research findings, or direct quotes from experts. Reliable information is usually well-supported by evidence that can be independently verified.



Ethical Media Consumption

Ethical media consumption involves being mindful of the media choices we make and the impact those choices can have on individuals and society. It requires a critical approach to selecting and sharing media content, considering factors such as accuracy, bias, representation, and the potential effects on public discourse. Ethical media consumers are proactive in seeking diverse perspectives, questioning the intent behind media messages, and avoiding the spread of unverified or harmful content.

To consume media ethically, it is important to understand the influence of algorithms on the media we encounter. Algorithms on social media platforms and search engines often personalise content based on your behaviour, creating echo chambers that reinforce your existing beliefs and limit

exposure to differing viewpoints. By being aware of these influences, you can take steps to diversify your media consumption, such as following sources with different perspectives, using tools that track media bias, or deliberately seeking out content that challenges your assumptions.

Responsible Content creation

As a creator, you should be mindful of the potential impact of your content, considering how it might affect various audiences, particularly vulnerable or marginalised groups. This includes avoiding language or imagery that perpetuates stereotypes, making sure you are accurate, and being respectful of individuals' privacy and consent in media portrayals. For example, when creating content that features real people, it is important to obtain consent and provide context to avoid misrepresentation.

Media literacy is an essential skill set for thriving in today's complex media environment. By fostering the ability to critically engage with media messages, recognise and manage misinformation, and create content ethically, you can empower yourself and others to navigate the media landscape with confidence and integrity. As the media continues to evolve, the principles of media literacy will remain vital in promoting a more inclusive, fair, and critically engaged society.

V. RESPONSIBLE SOCIAL MEDIA USE

According to the data about 97% of 16-29 year-olds in the EU used the Internet daily, and 83% used social media platforms in 2023 (Eurostat, 2023). Since the use of digital platforms is widespread among young people, you should understand the advantages and disadvantages of social media use.

Benefits of Social Media

The online culture enables the connection and communication with other digital citizens, and by building social capital, social media platforms can improve well-being. It also provides an environment to expand your interests, knowledge and skills, as well as for entertainment and support.

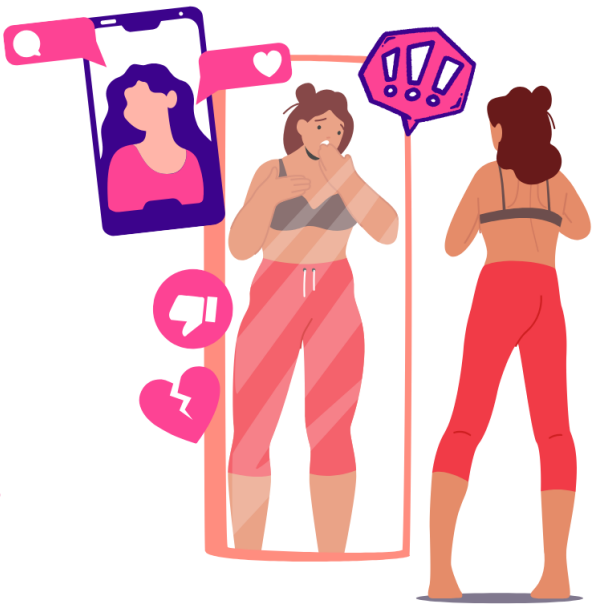
Moreover, it also helps you be informed about what is happening across the world. Many news channels have profiles on social platforms, where they share the most important news in a concise and comprehensible form, which makes it easy to stay up-to-date.

Social media can be particularly useful for youngsters in need – the online environment simplifies access to professional help, while preserving anonymity. In addition, via friends, and like-minded people in online groups, you can receive immediate emotional support. Social media also diminishes feelings of loneliness and isolation. Online communities that are moderated by mental health care professionals are exceptionally valuable – they create a safe environment for sharing emotions and receiving peer support. Some bloggers and influencers talk about mental health issues and offer space where individuals can share their testimony. Following someone's recovery story can make you feel encouraged to overcome your struggles.

Risks of Social Media

While acknowledging the benefits of social media, you should be aware of various pitfalls on the Internet that can pose a risk and threat. Statistically speaking, the risk exposure rises with the frequency of the online presence and intensity of the engagement. An array of factors, including age, gender, education and cultural background, influence the level of vulnerability to risks and their ramifications.

With the increased use of communication tools, social media, and gaming platforms, you are at risk of online harassment, cyberbullying, cyberstalking, flaming, hate speech, grooming, as well as identity theft. The virtual world also contains diverse harmful content of violent or sexual nature, disinformation, racism, antisemitism and much more, which has serious repercussions on the mental health of the young demographic and society as a whole.



Furthermore, teenage girls are especially vulnerable to being hurt online due to the social comparison of physical attractiveness and false beauty standards. Social media are swarming with pictures where individuals use beautifying filters and retouching to create unrealistic images of perfect bodies and faces. Due to the high exposure to such content, women are vulnerable to body image dissatisfaction and negative self-perception, which is further linked to low self-esteem and can result in mental health issues or eating disorders.

Subsequently, cool posts from events, vacations and festivals can trigger the fear of missing out (FOMO), and feelings of jealousy and own insufficiency.

We all often forget to take into account that many of these posts are staged and do not mirror the real lives of the users.

The entertainment of online platforms allows you to "escape" the real world. By chasing dopamine, you, as a digital citizen, are often overconsuming online content, which might result in online addiction. Such behaviour is time-exhausting and has a negative impact on your physical health, social relationships, concentration and productivity, which in turn can result in poor academic or working performance. Subsequently, it causes psychological discomfort and health repercussions. Social media is also associated with sleep disruption and anxiety.

Furthermore, you should be aware that not everything online is true, and that many profiles share misinformation or even disinformation, which can be very dangerous if taken seriously.

Controversial Aspects of Social Media: The Role of Algorithms

Algorithms, as a set of rules, calculations, and decision-making processes that platforms use to sort, recommend, and present content to users, are designed to prioritise content that users are most likely to interact with, based on previous behavioural data such as likes, shares, and time spent on specific content.

One positive aspect of social media algorithms is the enhanced user experience, as content is personalised, reducing information overload and promoting relevant information for the user. For instance, algorithms help you find communities and information tailored to your interests, making platforms more user-friendly.

However, one major concern is the reinforcement of echo chambers, where you are exposed primarily to content that aligns with your existing views. Algorithms prioritise sensational content, amplifying mis- and disinformation, as it increases engagement. If you are unaware of these manipulations, you

can easily fall into echo chambers that reinforce biases and promote misinformation, which can lead to polarisation and radicalisation.

The psychological effects of these algorithms are also profound. Constant exposure to emotionally charged content can lead to anxiety, depression, and feelings of isolation. Additionally, the addictive nature of algorithm-driven platforms contributes to social media overuse, where you find yourself in endless cycles of scrolling without realising the emotional toll it takes.

The effects of the European legislation on digital services requiring the platforms to disclose their recommender algorithms are yet to be seen.

The Conscious Click: Tips for Responsible Social Media Use

The online space should be safe and secure and make every user feel comfortable. People often use social platforms for socialising, professional networking, or activism, but the way they engage online can have lasting impacts on both their personal lives and society. Competences such as critical thinking, empathy and digital, media and information literacy are vital for social media use in the digital citizenship framework. To become responsible digital citizens, you should follow these tips:

- **Think before you post:** Social media often encourages impulsive posting. Posts made in anger or frustration may reflect poorly on your character and could be misinterpreted by others. A conscious approach to sharing can prevent misunderstandings or damage to your e-reputation.

- **Understand the consequences of sharing personal information**: Sharing personal data, such as PII (Personal Identifiable Information), location, travel plans, or sensitive opinions, can put you at risk. These posts can be used to track your activities, compromise your privacy, or even lead to identity theft.
- **Be aware of potential criminal activities:** It is vital to stay vigilant against both technological and human risks in the digital space. Recognise and avoid phishing and identity theft attempts as well as cyber-attacks. Avoid clicking on unknown or suspicious links and downloading files from untrusted sources.
- **Fact-check before sharing:** Before sharing articles or posts, ensure they come from credible sources. You should develop critical thinking skills to discern factual content from rumours or clickbait. Inaccurate or misleading posts not only damage your credibility but also contribute to social harm.
- **Maintain respect and empathy in online interactions:** Social media can be a space for healthy and constructive dialogue. Avoid engaging in online arguments or personal attacks, as these often escalate quickly and leave lasting negative impressions. Practise digital empathy and listen to opposing viewpoints respectfully, as it fosters a positive online environment.
- **Employ active and positive engagement:** Your digital reputation can be enhanced through thoughtful contributions. Whether in professional forums or social media, contributing valuable insights and practising digital empathy can help shape a strong, positive digital identity. This includes engaging in valuable discussions, sharing meaningful content, or supporting initiatives that promote inclusivity and social responsibility online.
- **Consider your audience**: Social media is often public or semi-public, and the audience may be broader than anticipated. Posts meant for your friends can easily reach future employers, academic institutions, or unintended viewers. Maintaining a representative, decent and respectful tone and employing netiquette can safeguard your e-reputation.

- **Avoid overconsumption of social media:** Limit social media consumption by being mindful of your screen time. Many smartphones now allow users to set time limits for apps, including social media, and send notifications when the limit is exceeded. This feature helps manage screen time and encourages awareness of potential overuse.

E-Reputation: How to Communicate and Present Yourself Online

The way you are perceived online, known as your e-reputation, is a direct reflection of your e-presence. E-presence is closely tied to online safety and ethical behaviour in virtual environments. The online presence extends beyond passive online participation; it involves actively cultivating a digital footprint through interactions, content creation, and ethical behaviour, emphasising the importance of digital literacy and self-awareness in shaping your public persona.

Your online identity can be formed both intentionally and unintentionally. The intentional creation of the identity involves the profile, pictures, posts, and personal information that you decide to put online. The unintentional features of your identity are established by someone else who uploads something about you, for instance, a tag in a picture or a post. Nowadays the platforms notify you that you have been tagged and provide the possibility to deny or confirm the tag. This option gives you some level of control over your indirect online identity.

Everything shared online leaves a trace, so it is essential to be conscious about what will be shared and its potential implications. The digital reputation you create can be easily reviewed through online searches of your name or other personally identifiable information (PII). The search results can include social media posts, comments, professional profiles, or any public content associated with your identity. Positive online presence, such as professional achievements or constructive engagement in forums, enhances your reputation. On the other hand, negative content, like inappropriate social media behaviour, controversial comments, or sharing misinformation, can harm your image and have a negative impact on future career opportunities. For instance, work and university applications can be dismissed due to the initial online social screening of the candidates.

VI. UNDERSTANDING AND MANAGING YOUR DIGITAL FOOTPRINT

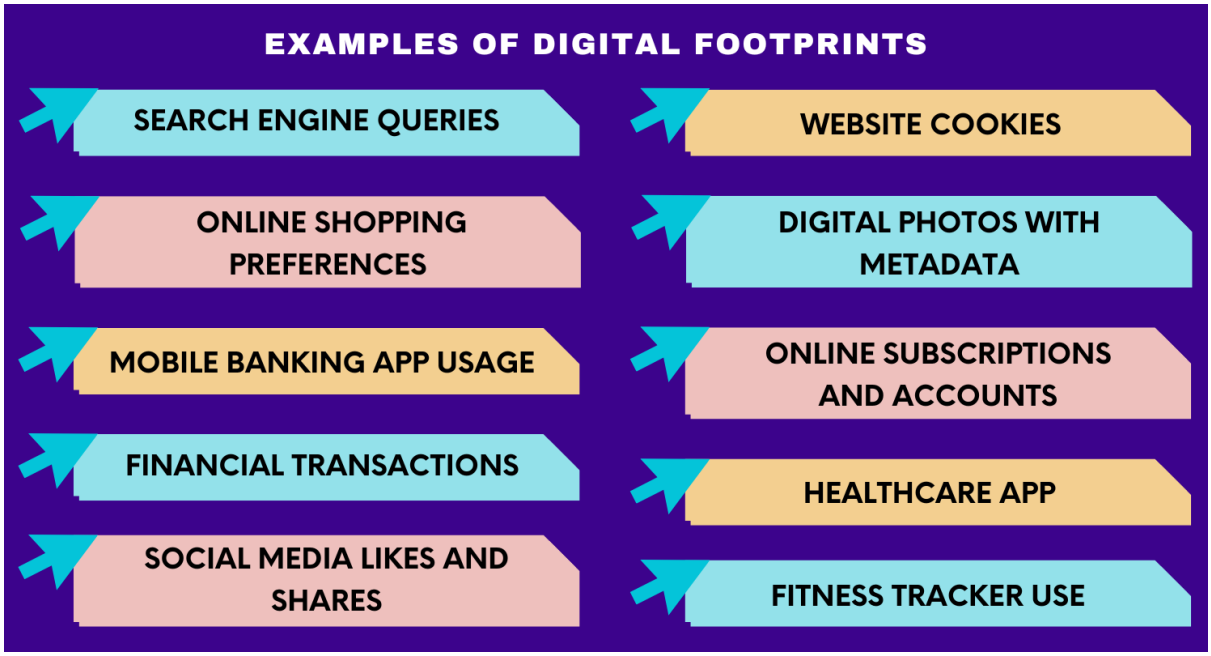
In today's interconnected world, our online activities leave behind a trail of data known as a digital footprint.

A digital footprint refers to the data trace you create while using the Internet. It includes all the information about your online activities, interactions, and presence across various digital platforms. You can encounter two types of digital footprints – active and passive.

An active digital footprint refers to the data that you intentionally share online, which you are aware of and control. This includes any information you deliberately post or submit, such as social media posts (on platforms like Facebook, X, or Instagram), online reviews you write for products or services, and account registrations, including information submitted when creating accounts on various websites.

A passive digital footprint is information collected about you without your direct involvement. It includes browsing history logged by websites, IP address records, location data from mobile devices, and data collected by apps running in the background.

Every action you do online leaves traces and sometimes digital footprints can be where you don't expect. Here are some examples of digital footprints so that you can be more aware of them:



The link between a digital footprint and e-reputation is significant, as the digital footprint forms the foundation of one's e-reputation. As we said above, a digital footprint encompasses all the data and traces left by an individual's online activities, both intentional and unintentional. This includes social media posts, comments, online purchases, and browsing history, among others.

An individual's digital footprint directly impacts their e-reputation because it reflects their values, interests, and behaviours. Potential employers, business partners, and even personal acquaintances often assess a person's e-reputation by examining their digital footprint. A positive digital footprint can enhance your professional and personal image, showcasing expertise and reliability. Conversely, a negative digital footprint, such as inappropriate content or controversial opinions, can damage credibility and trustworthiness, leading to lost opportunities.

Managing your digital footprint is crucial for maintaining a favourable e-reputation. This involves being mindful of the content shared online, utilising privacy settings, and regularly monitoring your online presence to ensure it aligns with desired personal and professional images.

Potential Pitfalls

Unmanaged digital footprints can lead to various risks besides negative e-reputation:

- **Privacy risks:** Digital footprints can expose you to privacy risks, including cyberstalking, harassment, and even physical threats. Personal information shared online can be used maliciously by others, leading to unwanted attention and potential harm.
- **Security threats:** Cybercriminals can exploit digital footprints for identity theft, phishing scams, and account spoofing. Exposed personal information, such as usernames and passwords, can be used to gain unauthorised access to your accounts, leading to financial loss and other damages.
- **Targeted advertising and data exploitation:** Companies use digital footprints to track user behaviour and preferences, enabling targeted advertising. While this can enhance user experience, it also raises concerns about data privacy and the extent to which personal information is used without explicit consent.
- **Environmental impact:** The storage and processing of digital data contribute to energy consumption and carbon emissions. Being mindful of your digital footprint can help mitigate environmental impacts.

The Environmental Aspect

The environmental aspect of digital footprint is an increasingly important consideration as our online activities continue to grow. Digital activities require significant energy consumption because data centres and networks that power online services account for approximately 1% of global energy-related greenhouse gas emissions.

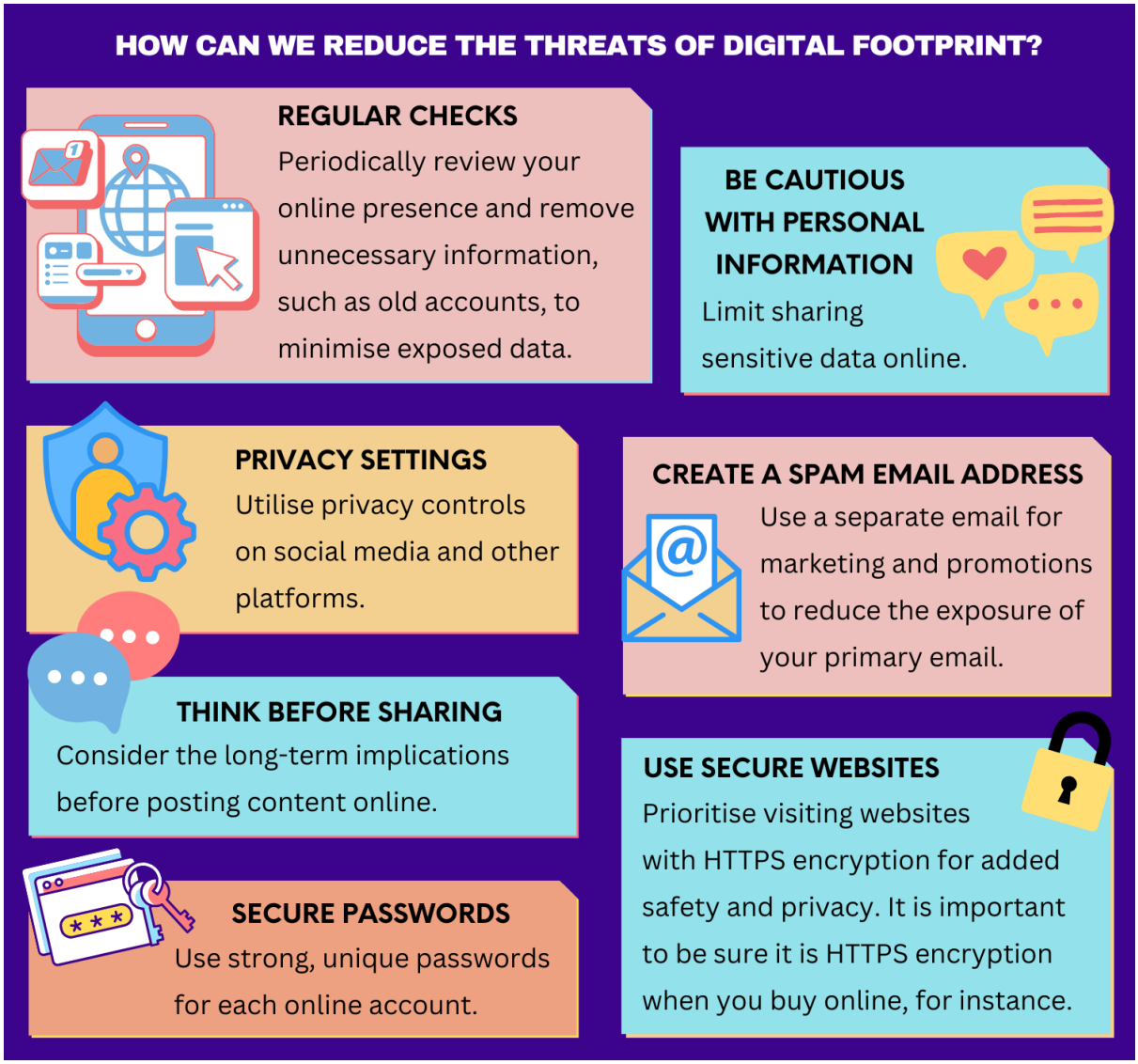
Moreover, the carbon footprint of digital content consumption is substantial. As digital services and technologies like cloud gaming, blockchain, and virtual reality grow, the environmental impact of digital footprints is expected

to rise sharply. To address these environmental concerns, experts recommend promoting digital sobriety practices to reduce unnecessary digital consumption, among other strategies.

In conclusion, understanding and managing the environmental aspect of digital footprints is crucial for ensuring a more sustainable digital future.

How Can We Reduce the Threats of Digital Footprint?

Managing your digital footprint starts with managing your personal data. The following tips can help you reduce the risks of your personal data being leaked:



Another useful tip is being familiar with the following tools and what they can do for you:

- **VPNs (Virtual Private Networks):** Mask your IP address and encrypt your online activities.
- **Ad blockers:** Reduce tracking by blocking advertisements and trackers.
- **Secure browsers:** Use browsers with built-in privacy features.
- **Privacy-focused search engines:** Choose search engines that don't track your queries.
- **Data removal tools:** Use services that help remove your personal information from data broker websites.
- **Secure networks:** Ensure your home Wi-Fi is protected to reduce the risk of exposure.
- **Software updates:** Regularly update your devices' software and antivirus programs.

By understanding your digital footprint and implementing these strategies, you can better protect your online presence and mitigate potential risks associated with your digital activities.

Keeping It Safe: Why Protecting Personal Information is Essential

Sensitive information such as names, addresses, identification numbers, financial data and even preferences and habits has become a valuable commodity, not just for individuals but also for corporations, third-party entities, and inevitably criminals. Protecting personal information is crucial to avoid privacy violations like identity theft and other malicious activities that stem from data breaches. Data breaches have become more frequent, meaning you should understand how your personal data is collected and stored, as well as the risks involved when it is inadequately protected (Council of Europe 2019).

The right to privacy is a fundamental human right, and its importance has become more pronounced in the modern digital environment. In 2018, the European Union's General Data Protection Regulation (GDPR) was introduced to regulate the collection, storage, and use of personal data (Sharma 2022). This legislation provides people with greater authority over their personal information, allowing them to manage their digital presence more effectively.

Risks of Personal Data Exposure

In many instances, users are unaware of the risks posed by data sharing. Seemingly innocent actions, such as posting a photo or sharing a location on social media, can inadvertently reveal more than intended and put you at risk.

The consequences of a personal data breach can be far-reaching and severe. One significant threat is identity theft, where malicious people steal and use sensitive personal data like identification numbers, login credentials or financial information for unauthorised buying or opening accounts in the victim's name. An additional risk is that someone can create a fake social media profile impersonating you, which has several negative consequences. The imposter may do something illegal, damaging your reputation by deceiving your friends, family, or colleagues. Additionally, such accounts can lead to the invasion of privacy, exposing personal information and contacts. This could also enable phishing attacks or identity theft, where the imposter uses the fake profile to gain unauthorised access to sensitive data, financial accounts, or other online platforms, causing you serious harm.

Furthermore, leaked personal data can lead to reputation damage, especially when personal information is exposed in inappropriate contexts or misused by third parties. If sensitive personal information, such as private messages, photos, or videos, is exposed online, it can be used to harm an individual's reputation, which damages personal and professional relationships, and it can also result in, for instance, harassment or

cyberbullying. In extreme cases, personal data leaks can escalate to real-world threats, such as stalking or extortion.

Moreover, privacy breaches may cause emotional distress, leaving victims feeling vulnerable, violated, and fearful of the potential repercussions. This psychological toll can severely affect individuals' well-being, mental health, and sense of security. The violation of privacy often leads to feelings of helplessness, as victims realise, they no longer have control over their personal information. This loss of control can result in heightened anxiety, stress, and a constant state of fear about what might happen next. Victims may experience insomnia, paranoia, or depression, as the breach can erode their trust in digital systems and others around them. This distress intensifies when the consequences of the breach, such as financial fraud or identity theft, manifest. The feeling of vulnerability is exacerbated when sensitive information, such as private photos or correspondence, is exposed online. This exposure can lead to reputation damage, cyberbullying, harassment, and even physical safety threats. Mental health issues, such as post-traumatic stress disorder (PTSD), may also emerge, especially if sensitive data like medical records or intimate photos are exposed.

The impact on one's sense of security is also critical. Persons affected by privacy breaches often feel unsafe in both their digital and physical environments, fearing further exploitation or harm. This lack of security can lead to social withdrawal, as victims avoid digital spaces and reduce their interactions to minimise further exposure. The psychological burden, therefore, is not limited to the moment of the breach but can extend far beyond, affecting various aspects of daily life.

To avoid such outcomes, it is crucial to recognise the importance of protecting personal information and take appropriate measures to mitigate

these risks. Digital citizens must take efficient measures to ensure that their private personal information will not be unauthorised, accessed and misused.

Stay Safe Online: Practical Tips for Maintaining Your Privacy

With personal data constantly at risk of exposure or misuse, it's important to understand and implement effective strategies for protecting it. Here are key practices to help individuals safeguard their privacy in the digital space:

Limit Information Sharing and Adjust Privacy Settings

Sharing personal information online should be done cautiously. You can unknowingly share more information than necessary, such as real-time locations or personal habits. Reducing the amount of personal data shared, whether on social media or other platforms, can help protect you against risks like cyberstalking or identity theft. For example, avoid posting travel itineraries or routine updates that could make you vulnerable to stalking or other malicious activities.

Adjusting privacy settings can also control who has access to personal data, mitigating the risk of unwanted exposure. It can be recommended to set the profile private, and not let strangers follow you. Additionally, creating a "close friends" list on platforms like Instagram or using Facebook's privacy settings to limit the visibility of posts can help prevent unwanted exposure.

Regularly Update Privacy Settings

As technology and privacy practices evolve, it is important to regularly review and update the privacy settings of your apps and online accounts. This ensures that personal data is shared according to your preferences. You should also disable location-sharing features or revoke unnecessary permissions from apps and services that no longer need access to your data.

Stay Informed About Data Privacy Laws

GDPR has been introduced to protect individuals' data privacy by ensuring websites obtain explicit consent before collecting personal information. Staying informed about such laws allows you to better understand your rights and take control of your digital footprint. For instance, GDPR gives users the right to request that their data be deleted or not shared with third parties.

Manage Cookies and Browser Settings

Cookies, small pieces of data stored on users' devices, are used by most websites and are typically enabled by default in web browsers. You can modify their settings to accept or reject cookies.

While some cookies are essential for website functionality, others can track your activity across different sites. Managing cookie preferences in your browser settings can help you control which types of cookies are allowed, thereby limiting unnecessary tracking. Additionally, periodically clearing cookies and browsing data can help enhance privacy.

Develop Basic Technological Knowledge

Having a basic understanding of technological concepts like encryption, cookies, and IP addresses can go a long way in protecting your online privacy. For example, knowing how encryption works can help you choose secure communication methods, and understanding IP addresses can make you more aware of how your location might be tracked online. Learning about privacy-enhancing technologies, such as VPNs and secure browsers, can also empower you to protect your data more effectively and to increase your anonymity online.

Be Cautious with Public Wi-Fi and Shared Devices

Public Wi-Fi, though convenient, poses a significant security risk due to its lack of encryption. This makes it easier for cybercriminals to intercept personal data. To stay safe while using public Wi-Fi, avoid conducting sensitive transactions such as online banking or shopping. A more secure alternative is to use a VPN, which encrypts your Internet connection and protects your

data from being intercepted by other people. Similarly, using public or shared devices, such as computers in the university library, poses security risks. Personal data, such as login credentials or browsing history, can be inadvertently stored and accessed by subsequent users.

Use Strong Passwords and Two-Factor Authentication (2FA)

One of the most straightforward ways to protect online accounts is by using strong, unique passwords. A strong password typically combines uppercase and lowercase letters, numbers, and special characters. It's also critical to avoid reusing passwords across different platforms. Two-factor authentication (2FA) adds an extra layer of security, requiring a second form of identification, such as a text message code or authentication app, which significantly reduces the chances of unauthorised access.

Use Secure Websites (HTTPS)

When sharing personal information or shopping online, always ensure the website is secure by checking for the HTTPS prefix in the URL. The "S" in HTTPS stands for "secure," indicating that the website uses encryption to protect the data being intercepted by third parties. Look for the padlock or toggle icon next to the URL to verify that the connection is secure.

By implementing these practical tips, you can significantly enhance your privacy and security online, which is not just a necessity but a responsibility. Through a combination of proactive privacy management and technological awareness, you can minimise the risks associated with sharing personal data online.

VII. CONCLUSION

As the digital world becomes increasingly central to our daily lives, equipping young people with the skills and values of digital citizenship has never been more critical. According to Eurostat (2023), 97% of individuals aged 16 to 29 in the EU used the Internet daily, and 83% were active on social media. These statistics highlight the pervasive role of digital technologies in shaping how young people learn, connect, and engage with the world.

The digital space serves as a "window to the world," offering opportunities to acquire new knowledge and skills. However, to fully leverage these opportunities while navigating potential risks, young people need a strong foundation in digital citizenship. This guide, aligned with the European Commission's Digital Competences Framework for Citizens, provides that foundation by emphasising critical thinking, ethical behaviour, and essential competencies for the future.

Digital citizenship encompasses more than just technical know-how; it is about fostering informed, respectful, and responsible participation in digital environments. By integrating principles of online privacy, media literacy, responsible social media use, and the management of digital footprints, this guide equips learners to make thoughtful decisions and contribute positively to the digital community.

The competencies outlined in this guide are not only vital for navigating today's digital landscape but are also essential for future success in an increasingly digitalised world. As educators, trainers, and organisations implement these practices, they will help shape a generation capable of addressing the challenges and maximising the opportunities of the digital age.

Together, let us continue to promote digital citizenship as a cornerstone of education, ensuring that young people can safely, ethically, and effectively explore the limitless possibilities of the digital world.

GLOSSARY

Account spoofing	The act of impersonating or faking a legitimate account or identity in order to deceive others.
Artificial intelligence (AI)	The simulation of human intelligence in machines that are programmed to think, learn, and perform tasks typically requiring human cognition, such as understanding language, recognising patterns, solving problems, and making decisions.
Augmented reality (AR)	Technology that overlays digital information, such as images, sounds, or other data, onto the real-world environment in real time.
Author's credentials	The qualifications, experience, education, and expertise that an individual possesses in relation to the subject they are writing about.
Bias	A tendency or preference that affects an individual's judgment, perception, or behaviour in a way that is unfair, skewed, or one-sided.
Copyright law	A legal framework that grants creators of original works exclusive rights to use, reproduce, distribute, and adapt their creations.
Critical evaluation	The process of carefully assessing and analysing something—whether it is an idea, argument, work, theory, or source of information—by examining its strengths, weaknesses, relevance, accuracy, and overall validity.

Critical thinking	The process of actively and objectively analysing, evaluating, and synthesising information to make reasoned and well-informed decisions or judgments.
Cyberbullying	The use of digital technology to harass, threaten, humiliate, or harm someone.
Cyberstalking	The use of the Internet, social media, or other online platforms to stalk or harass an individual or group.
Digital	Anything involving the representation, storage, or processing of information in discrete, binary formats (e.g., 0s and 1s) as opposed to continuous, analogue signals. Digital technology is foundational to modern computing and telecommunications.
Digital addiction	The excessive and compulsive use of digital technologies, such as smartphones, computers, social media, video games, or the Internet, to the point where it negatively impacts various aspects of a person's life, such as relationships, work, health, or overall well-being.
Digital citizen	An individual who uses digital technologies and the Internet responsibly, ethically, and effectively to engage in society, politics, education, and culture.
Digital citizenship	The responsible, ethical, and informed use of technology, particularly the Internet, to participate effectively in society.
Digital commerce / e-commerce	The buying and selling of goods and services over the Internet.

Digital community / online community	A group of people who interact, share, and collaborate through digital platforms and online spaces.
Digital competence	The set of skills, knowledge, and attitudes required to effectively and responsibly use digital technologies in various aspects of life, including personal, educational, and professional contexts.
Digital content	Any information or material that is created, stored, distributed, or consumed in a digital format.
Digital environment	Any virtual space or ecosystem where digital interactions, activities, or processes occur.
Digital footprint	The trail of data or information that a person leaves behind when they use digital devices, interact online, or engage with technology.
Digital literacy	The ability to effectively, safely, and responsibly use digital technologies, tools, and platforms to access, evaluate, create, and communicate information.
Digital problem-solving	The ability to use digital tools, technologies, and resources to identify, analyse, and find solutions to problems or challenges in various contexts, such as work, personal life, or education.
Digital rights	The rights and freedoms individuals have in the digital world, including their ability to access, use, create, and share digital content and information while also protecting their personal data and privacy.
Digital skills	The ability to use technology tools and platforms effectively.

Digital space	Any environment or platform that exists online or is powered by digital technologies, where users interact, communicate, and engage with content, services, or each other.
Digital storytelling	The practice of using digital tools and platforms to create and share stories.
Digital tools	Software, platforms, applications, or devices that use digital technology to perform tasks, solve problems, communicate, or facilitate activities.
Digital world	The global ecosystem created by digital technologies, where information, communication, and activities take place through electronic and online means.
Disinformation	Deliberately false or misleading information that is spread with the intention to deceive or manipulate others.
Echo chambers	Environments, typically within media or social networks, where individuals are exposed primarily to information, opinions, or ideas that reinforce their existing beliefs or viewpoints rather than challenging them with diverse perspectives.
Email (electronic mail)	A method of exchanging digital messages between people using electronic devices, primarily over the Internet.
Empathy	The ability to understand, share, and relate to the feelings, thoughts, or experiences of another person.
Equity	The principle of fairness and justice in the distribution of resources, opportunities, and treatment, ensuring that

	individuals or groups receive what they need to achieve equality of outcomes.
Fact-checking	The process of verifying the accuracy and truthfulness of information, claims, or statements, typically by cross-referencing them with reliable, credible sources.
Flaming	The act of posting or sending offensive, inflammatory, or insulting comments online with the intention of provoking others, inciting anger, or starting conflicts.
General Data Protection Regulation (GDPR)	A comprehensive data protection law enacted by the European Union (EU). It came into effect on May 25, 2018, and is designed to regulate the processing of personal data of individuals within the EU and European Economic Area (EEA).
Grooming	The process by which an individual builds a relationship with a child or vulnerable person to manipulate, exploit, or abuse them.
Identity theft	The unauthorised acquisition and use of someone else's personal information, typically for fraudulent purposes.
Inclusion	The practice of creating environments, systems, and communities that embrace diversity and ensure that all individuals, regardless of their background, identity, or abilities, have equal access to opportunities, participation, and respect.
Information literacy	The ability to locate, evaluate, and use information effectively, efficiently, and ethically.

Intellectual property rights	The legal protections granted to creators and owners of intellectual property (IP), which includes intangible creations of the mind.
Media literacy	The ability to access, analyse, evaluate, and create media in various forms.
Misinformation	False or inaccurate information that is spread, regardless of intent to deceive.
Online activism	The use of digital tools and platforms to advocate for social, political, environmental, or economic causes.
Online exploitation	The act of using the Internet or digital platforms to take unfair advantage of individuals, often through manipulation, coercion, or deception, for personal, financial, or sexual gain.
Online harassment	The use of digital platforms and technology to intentionally harm, intimidate, threaten, or belittle an individual or group.
Participation	The active involvement or engagement of individuals in activities, decision-making processes, or events.
Personal information or Personal identifiable information (PII)	Any data or information that can be used to identify, contact, or locate an individual, either directly or indirectly.
Phishing	A type of cyberattack in which attackers impersonate legitimate institutions or individuals to trick people into revealing sensitive information, such as passwords, credit

	card numbers, social security numbers, or other personal data.
Podcast	A digital audio or video program that can be streamed or downloaded from the Internet, typically in a series of episodes.
Social capital	A concept used to describe the value derived from social interactions and the connections people have within their communities, organisations, or societies.
Social media	Digital platforms and applications that enable users to create, share, and exchange content, ideas, and information with others through virtual communities and networks.
Streaming services	Platforms or technologies that allow users to access and consume media content (such as music, videos, TV shows, movies, and live broadcasts) over the Internet in real-time, without needing to download the content first.
Virtual reality (VR)	A computer-generated simulation of an environment that immerses users in a completely virtual world, typically through the use of a headset, sensors, and sometimes additional equipment like gloves or controllers.

BIBLIOGRAPHY

All images retrieved from **Canva**.

Aboujaoude, E. (2022). "Protecting Privacy to Protect Mental Health: The New Ethical Imperative". *Journal of Medical Ethics*. **https://doi.org/10.1136/medethics-2018-105313**

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., & Diaz, C. (2014). "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild". *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 674-689. **https://dl.acm.org/doi/10.1145/2660267.2660347**

Baltacı, Ö., Bektas, M., & Kutlu, F. (2021). "Internet addiction, social anxiety, and coping strategies among university students: A cross-sectional study". *Journal of Research in Adolescence*, 31(3), 565-575.

Better Internet for Kids. (2020). *Insafe insights on...online reputation*. **https://www.betterinternetforkids.eu/practice/awareness/article?id=6668871**

Bucher, T. (2018). "If...Then: Algorithmic Power and Politics". *Oxford Studies in Digital Politics, New York, 2018; online edn, Oxford Academic*. **https://doi.org/10.1093/oso/9780190493028.001.0001**

Carrascal, J.P., et al. (2013). "Your Browsing Behavior for a Big Mac: Economics of Personal Information Online." *Computers in Human Behavior*, vol. 29, no. 2, 2013, pp. 340–349. **https://arxiv.org/abs/1112.6098**

Cataldo, I., Lepri, B., Neoh, M. J.-Y., & Esposito, G. (2021). "Social media usage and development of psychiatric disorders in childhood and adolescence: A review". *Frontiers in Psychiatry, 11*. **https://doi.org/10.3389/fpsyt.2020.508595**

Cyber Citizenship. (2023). *Digital Citizenship 101: Responsible Online Behavior*. **https://www.cybercitizenship.org/digital-citizenship-guide/**

ENISA. (2017). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*. **https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines**

eSafety Commissioner. (2024). *Digital reputation*. **https://www.esafety.gov.au/key-topics/staying-safe/digital-reputation**

European Data Protection Supervisor. (2020). Guidelines on the Protection of Personal Data. **https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en**

Eurostat. (2024). *Young people - digital world.* **https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/39761.pdf**

Fardouly, J., Magson, N. R., Rapee, R. M., Johnco, C. J., & Oar, E. L. (2020). "The use of social media by Australian preadolescents and its links with mental health". *Journal of Clinical Psychology*, *76*(7), 1304–1326. **https://doi.org/10.1002/jclp.22936**

Gillespie, T. (2018). "Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media". *Yale University Press*. **http://dx.doi.org/10.12987/9780300235029**

Helberger, N. (2020). "The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power". *Digital Journalism*, *8*(6), 842–854. **https://doi.org/10.1080/21670811.2020.1773888**

Isin, E., & Ruppert, E. (2015). *Being Digital Citizens.* Rowman & Littlefield International, Ltd. ISBN/9781786614490. **https://rowman.com/WebDocs/Being_Digital_Citizens_Second_Ed_Open_Access.pdf**

Kaspersky. (2024). *What is a Digital Footprint?*. **https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint**

Kotobee Blog. (2024). *Game-Based Learning: What It Is and How to Apply It*. **https://blog.kotobee.com/game-based-learning/**

Kozyreva, A., Wineburg, S., Lewandowsky, S., Hertwig, R. (2022). "Critical Ignoring as a Core Competence for Digital Citizens." *Current Directions in Psychological Science* 32 (1): 81–88. Crossref. **https://journals.sagepub.com/doi/full/10.1177/09637214221121570**

Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final report 2009.* EU Kids Online Network. **http://eprints.lse.ac.uk/24372/**

McCrae, N., Gettings, S., & Purssell, E. (2017). "Social media and depressive symptoms in childhood and adolescence: A systematic review". *Adolescent Research Review*, 2, 315–330. **https://doi.org/10.1007/s40894-017-0053-4**

Netsafe. (2018). *From literacy to fluency to citizenship: Digital citizenship in education (2nd ed.)*. Wellington, NZ. **https://www.researchgate.net/publication/332886585**

Nolan, S., Hendricks, J., Ferguson, S., & Towell, A. (2017). "Social networking site (SNS) use by adolescent mothers: Can social support and social capital be enhanced by online social networks? – A structured review of the literature". *Midwifery*, 48, 24–31. **https://doi.org/10.1016/j.midw.2017.03.002**

OECD. (2022). *Is digital media literacy the answer to our disinformation woes?* The OECD Education Podcast. **https://www.oecd-ilibrary.org/education/is-digital-media-literacy-the-answer-to-our-disinformation-woes_326b63bf-en**

Oxford Dictionary. (n.d.). *Definition of 'digital citizenship.* **https://dictionary.cambridge.org/dictionary/english/digital-citizenship**

Popat, A., & Tarrant, C. (2023). "Exploring adolescents' perspectives on social media and mental health and well-being – a qualitative literature review". *Clinical Child Psychology and Psychiatry*, 28, 323–337. **https://doi.org/10.1177/13591045221092884**

Pretorius, C., Chambers, D., & Coyle, D. (2019). "Young People's Online Help-Seeking and Mental Health Difficulties: Systematic Narrative Review". *Journal of medical Internet research*, *21*(11), e13873, **https://doi.org/10.2196/13873**

Richardson, J., & Milovidov, E. (2019). *Digital citizenship education handbook*. Council of Europe. **https://rm.coe.int/16809382f9**

Ringrose, J., Gill, R., Livingstone, S. & Harvey, L. (2012). "A qualitative study of children, young people and 'sexting': A report prepared for the NSPCC". London: NSPCC. **https://www.researchgate.net/publication/265741962**

Sala, A., Porcaro, L., & Gómez, E. (2024). "Social Media Use and adolescents' mental health and well-being: An umbrella review". *Computers in Human Behavior Reports*, *14*, 100404. **https://doi.org/10.1016/j.chbr.2024.100404**

Scheinin, M. (2009). "Law and Security: Facing the Dilemmas". *SSRN Electronic Journal*. **http://dx.doi.org/10.2139/ssrn.1555686**

Secure Privacy. (2022). *The Ultimate Guide to Cookie Consent*. **https://secureprivacy.ai/blog/the-ultimate-guide-to-cookie-consent**

Senekal, J. S., Groenewald, G. R., Wolfaardt, L., Jansen, C., & Williams, K. (2023). "Social media and adolescent psychosocial development: A systematic review". *South African Journal of Psychology*, 53, 157–171. **https://doi.org/10.1177/00812463221119302**

Sharma, A. (2022). "Teaching Digital Privacy: Navigating the Intersection of Technology, Education, and Privacy." *Kanpur Historians*. Vol. IX, Issue II. **https://www.researchgate.net/publication/381952547_Teaching_Digital_Privacy_Navigating_the_Intersection_of_Technology_Education_and_Privacy**

Sheldon, R. (2023). *Navigating the Digital World: Online Reputation and Online Etiquette*. Igniyte. **https://www.igniyte.com/blog/navigating-the-digital-world-online-reputation-and-online-etiquette/**

Techopedia. (2023). *How to Protect Your Privacy Online*. **https://www.techopedia.com/how-to/how-to-protect-your-privacy-online**

Twenge, J. M., Haidt, J., Lozano, J., & Cummins, K. M. (2022). "Specification curve analysis shows that social media use is linked to poor mental health, especially among girls". *Acta Psychologica*, *224*, 103512. **https://doi.org/10.1016/j.actpsy.2022.103512**

UNICEF. (2023). *Digital civic engagement by young people*. **https://www.unicef.org/innocenti/reports/digital-civic-engagement-young-people**

G, V. (2024, July 31). *How can your digital footprint affect you in business opportunities?* Reputation Sciences. **https://www.reputationsciences.com/how-can-your-digital-footprint-affect-you/**

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills, and attitudes*. Publications Office of the European Union. **https://data.europa.eu/doi/10.2760/115376**

Webster, D., Dunne, L., & Hunter, R. (2021). „Association between social networks and subjective well-being in adolescents: A systematic review". *Youth & Society*, 53, 175–210. **https://doi.org/10.1177/0044118X20919589**

Wolford B, (n.d.), *What is GDPR, the EU's new data protection law?*, GDPR.eu, **https://gdpr.eu/what-is-gdpr/**

DIGICITY

GAME-BASED
DIGITAL CITIZENSHIP

www.projectdigicity.eu

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the National agency Tempus Foundation. Neither the European Union nor the National agency Tempus Foundation can be held responsible for them.

Project code: 2023-2-RS01-KA220-YOU-000170562

LogoPsyCom PENS digiQ YuzuPulse