



Navigating AI and Internet Safety for Young Females & Mental Health – NAOMI

Digital Safety Guide

Project Number: 2024-3-FR02-KA210-YOU-000277850

www.naomi-project.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 Agence du Service Civique / Agence Erasmus + France Jeunesse & Sport. Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

Welcome to the Digital Safety Guide	03
Introduction	04
Chapter 1. Understanding the Digital World	06
Chapter 2. Common Online Risks and Threats	09
Chapter 3. Cyberbullying, Online Harassment and Digital Abuse	11
Chapter 4. Protecting Your Privacy and Personal Data	13
Chapter 5. Creating Strong Passwords and Securing Your Accounts	14
Chapter 6. Safe Social Media Practices	16
Chapter 7. Artificial Intelligence in Everyday Life	18
Chapter 8. Ethical AI: Opportunities, Risks and Bias	20
Chapter 9. Digital Well-being and Mental Health	22
Chapter 10. Building Healthy Digital Habits	23
Chapter 11. Responding to Online Risks and Seeking Support	25
Chapter 12. Useful Digital Safety Tools and Resources	27
Digital Safety Checklist	28
Final Thoughts: Becoming a Responsible Digital Citizen	29

Welcome to the Digital Safety Guide

Welcome to the NAOMI Digital Safety Guide, developed within the framework of the NAOMI – Navigating AI and Internet Safety for Young Females & Mental Health project.

In today's interconnected world, digital technologies have become an integral part of our everyday lives. They provide unprecedented opportunities for communication, education, creativity, and personal development. At the same time, the rapid advancement of the digital landscape presents new challenges that require awareness, critical thinking, and responsible online behaviour.

This guide has been designed to support young women in developing the knowledge, skills, and confidence needed to navigate digital environments safely, responsibly, and ethically. It serves as a practical resource, offering guidance on internet safety, digital privacy, responsible use of Artificial Intelligence, online well-being, and the protection of personal data in an increasingly technology-driven society.

Throughout these pages, you will discover practical advice, useful strategies, real-life examples, and recommendations that will help you recognise potential online risks, make informed digital decisions, protect your personal information, and cultivate healthier digital habits. The guide also encourages critical reflection on the role of Artificial Intelligence in everyday life, promoting ethical technology use and responsible digital citizenship.

Digital safety is not solely about protecting devices or accounts, it is about protecting yourself, your privacy, your mental well-being, and your rights in the digital world. By becoming more informed and digitally resilient, you can confidently benefit from the opportunities offered by technology while reducing the risks associated with online environments.

We hope this guide will become a valuable companion that you can revisit whenever you need practical advice, reassurance, or inspiration to make safer and more informed choices online. Together, let us build a digital world that is safer, more inclusive, more respectful, and empowering for everyone.

Introduction

The digital world has transformed the way we communicate, learn, work, and interact with one another. Digital technologies have become an integral part of our daily lives, shaping how we access information, build relationships, express creativity, participate in education, and engage with communities across the world. For young people in particular, digital environments provide countless opportunities for learning, collaboration, innovation, and personal development, allowing them to connect beyond geographical boundaries and actively participate in an increasingly interconnected global society.

At the same time, the rapid evolution of digital technologies has introduced new challenges that require awareness, critical thinking, and responsible decision-making. The increasing presence of social media platforms, online communities, Artificial Intelligence, and digital communication tools has created an environment where opportunities and risks coexist. Cyberbullying, online harassment, misinformation, privacy breaches, identity theft, online scams, digital manipulation, and excessive exposure to digital content are only some of the issues that can affect individuals' safety, well-being, and confidence in navigating the online world.

The emergence of Artificial Intelligence has further transformed digital experiences, influencing the information we consume, the content we create, and the decisions we make online. AI-powered recommendation systems, automated content generation, personalised advertisements, and intelligent digital assistants have become common features of everyday life. While these technologies offer remarkable opportunities for innovation and accessibility, they also raise important ethical questions concerning privacy, transparency, fairness, misinformation, and responsible technology use. Developing a clear understanding of these technologies has therefore become an essential component of digital literacy.

Young women, in particular, may encounter unique challenges within digital environments. Online harassment, cyberbullying, gender-based discrimination, unrealistic beauty standards, misinformation, unwanted contact, and increasing pressure to maintain an online presence can have a significant impact on emotional well-being and self-confidence.

Equipping young women with the knowledge, practical skills, and confidence to recognise these challenges and respond effectively is essential for promoting safer and more inclusive digital spaces. This Digital Safety Guide has been developed within the framework of the NAOMI – Navigating AI and Internet Safety for Young Females & Mental Health project to provide practical knowledge, evidence-informed guidance, and useful strategies that empower young women to navigate digital environments safely, confidently, and responsibly. Rather than focusing solely on potential risks, this guide encourages readers to view technology as a powerful tool for learning, communication, creativity, and social participation when used ethically and consciously.

Throughout the following chapters, you will explore the fundamental principles of digital safety, online privacy, responsible social media use, ethical Artificial Intelligence, cybersecurity, and digital well-being. You will discover practical recommendations for protecting your personal information, recognising online threats, critically evaluating digital content, understanding how Artificial Intelligence shapes your online experiences, and developing healthy digital habits that contribute to both your personal security and mental well-being.

In addition to practical advice, this guide encourages reflection on the role each of us plays in creating safer digital communities. Responsible digital citizenship extends beyond protecting ourselves; it also involves respecting others, promoting empathy and inclusion, combating misinformation, and contributing positively to the online spaces we share. Every informed decision we make has the potential to strengthen trust, safety, and respect within the digital world.

Digital literacy is no longer simply a technical competence, it is a fundamental life skill. As digital technologies continue to evolve, lifelong learning, adaptability, and critical thinking will become increasingly important. Strengthening these competences, you will be better equipped to make informed decisions, protect your rights and privacy, support your mental well-being, and confidently embrace the opportunities offered by today's digital society.

We hope that this guide will serve not only as a practical reference but also as a source of inspiration, encouraging you to become a confident, informed, and responsible digital citizen. Together, we can contribute to building digital environments that are safer, more respectful, more inclusive, and empowering for everyone.

Chapter 1. Understanding the Digital World

Digital technologies have become an inseparable part of modern society, fundamentally transforming the way individuals communicate, learn, work, access information, and participate in everyday life. Smartphones, computers, tablets, social media platforms, messaging applications, cloud-based services, and Artificial Intelligence have reshaped nearly every aspect of human interaction, making digital connectivity an essential component of modern living. Whether communicating with family and friends, attending online classes, managing professional responsibilities, accessing healthcare services, or participating in civic initiatives, digital technologies now influence many of our daily decisions and experiences.

The rapid expansion of digital innovation has created unprecedented opportunities for education, creativity, entrepreneurship, collaboration, and social participation. Through digital platforms, people can connect instantly across geographical boundaries, exchange ideas with individuals from diverse cultural backgrounds, collaborate on international projects, and access educational resources that were once limited by location or financial barriers. Information that previously required hours of research in libraries is now available within seconds, allowing individuals to continuously expand their knowledge and develop new skills throughout their lives.

For young women in particular, the digital world offers significant opportunities for personal and professional development. Online learning platforms provide access to specialised courses and professional certifications, while social media and digital communities create spaces where young women can share experiences, find inspiration, build supportive networks, and amplify their voices on issues that matter to them. Digital technologies also encourage creativity by providing opportunities to create content, launch entrepreneurial initiatives, participate in international communities, and develop valuable digital competences that are increasingly demanded in today's labour market.

Beyond education and employment, digital technologies have also transformed civic participation. Online platforms enable citizens to engage in public discussions, participate in awareness campaigns, volunteer remotely, advocate for social causes, and contribute to community initiatives regardless of geographical location. These opportunities strengthen democratic participation and encourage active citizenship in ways that were unimaginable only a few decades ago.

Despite these remarkable opportunities, the digital landscape is continuously evolving and becoming increasingly complex. Every interaction we have online leaves behind a digital footprint, a record of our online activities that may include websites visited, content shared, purchases made, search histories, location data, and interactions with other users. Much of this information is collected, analysed, and processed by digital platforms to personalise online experiences and improve digital services.

Artificial Intelligence plays a growing role in shaping these experiences. Recommendation algorithms determine which videos appear on our screens, which news articles receive greater visibility, which advertisements are displayed, and even which social media posts are prioritised within our personal feeds. Although these personalised experiences often improve convenience and accessibility, they also influence the information we consume, the opinions we encounter, and, in some cases, the decisions we make. Understanding these processes enables individuals to engage with technology more consciously rather than simply accepting algorithmic recommendations without reflection.

Developing a clear understanding of how digital platforms operate is therefore an essential component of digital literacy. Digital literacy extends far beyond the technical ability to operate electronic devices or navigate online platforms. It encompasses the knowledge, skills, and attitudes required to interact responsibly, safely, ethically, and critically within digital environments.

Being digitally literate means understanding how information is created, distributed, and consumed online. It involves recognising reliable sources of information, identifying misinformation and manipulation, protecting personal data, respecting the privacy and rights of others, and understanding the opportunities and limitations of emerging technologies such as Artificial Intelligence.

It also requires awareness of online risks, including cyberbullying, identity theft, phishing attacks, digital scams, and the potential emotional impact of excessive or unhealthy technology use. Equally important is the ability to think critically about digital content. The internet provides access to an enormous quantity of information; however, not all online content is accurate, objective, or trustworthy.

Developing critical thinking skills enables individuals to evaluate sources, question the credibility of information, recognise bias, and make informed decisions before accepting or sharing digital content. In an era characterised by rapidly evolving technologies and AI-generated information, these competences are becoming increasingly valuable.

Digital literacy also incorporates ethical responsibility. Every interaction in the digital world has consequences, whether posting a comment, sharing a photograph, creating content, or participating in online discussions. Respecting others, communicating responsibly, promoting inclusion, protecting personal privacy, and contributing positively to digital communities are fundamental characteristics of responsible digital citizenship. Technology should always be used in ways that promote cooperation, empathy, equality, and mutual respect.

Furthermore, digital competence includes understanding the relationship between technology and personal well-being. Maintaining a healthy balance between online and offline life, recognising when technology begins to negatively affect mental health, and developing healthy digital habits are increasingly recognised as essential aspects of digital literacy. Becoming digitally literate therefore means not only knowing how to use technology effectively but also understanding when and how to disconnect in order to preserve emotional well-being and maintain meaningful human relationships.

As digital technologies continue to evolve at an unprecedented pace, digital literacy must be viewed as a lifelong learning process rather than a skill that is acquired once and remains unchanged. Continuous learning, adaptability, curiosity, and openness to new technologies enable individuals to respond confidently to future digital challenges while taking advantage of the opportunities that innovation creates.

Ultimately, developing digital literacy empowers individuals to become active participants rather than passive consumers within the digital world. It provides the confidence to make informed decisions, protect personal privacy, recognise online risks, use Artificial Intelligence responsibly, and contribute positively to safe, inclusive, and respectful digital communities. In today's increasingly interconnected society, digital literacy is no longer simply a desirable competence, it is a fundamental life skill that enables every individual to thrive safely, responsibly, and confidently in the digital age.

Chapter 2. Common Online Risks and Threats

While the internet offers countless opportunities for communication, education, entertainment, and personal development, it also exposes users to a variety of potential risks that can affect their security, privacy, and overall well-being. As digital technologies continue to evolve, so do the methods used by individuals and organisations that seek to exploit vulnerabilities for malicious purposes. Developing an understanding of these challenges is the first step towards protecting yourself, making informed decisions, and navigating the online world with confidence.

One of the most widespread digital risks is cyberbullying, which involves repeated acts of harassment, intimidation, humiliation, or abuse carried out through digital platforms. Cyberbullying may occur on social media, messaging applications, online gaming platforms, discussion forums, or any other form of digital communication. Unlike traditional bullying, online abuse can occur at any time of day, reach a wide audience within seconds, and remain accessible for long periods of time, increasing its emotional and psychological impact. Victims may experience anxiety, stress, isolation, reduced self-esteem, or even long-term mental health consequences.

Another significant threat involves phishing attacks and online scams. Cybercriminals increasingly use sophisticated techniques to deceive individuals into revealing sensitive information, including passwords, banking details, personal identification data, or login credentials. These fraudulent attempts often appear as legitimate emails, text messages, social media communications, or websites that closely resemble trusted organisations. Developing the ability to recognise suspicious communications, verify sources, and avoid clicking on unknown links is essential for preventing identity theft, financial fraud, and unauthorised access to personal accounts.

Privacy breaches have also become an increasingly important concern in today's interconnected world. Every online interaction generates personal data, and sharing excessive information through social media, websites, or mobile applications may unintentionally expose individuals to identity theft, cyberstalking, unwanted contact, targeted advertising, or misuse of personal information. Even details that may appear harmless—such as photographs, location tags, travel plans, daily routines, or information about family members—can be combined to create detailed personal profiles that may be exploited for malicious purposes. Protecting personal data therefore requires careful consideration of what information is shared and with whom.

The rapid spread of misinformation and disinformation presents another major challenge within today's digital environment. False or misleading information can circulate quickly through social media platforms, messaging applications, and online communities, often influencing public opinion, personal decisions, and social behaviour. In some cases, misleading content is shared unintentionally, while in others it is deliberately created to manipulate audiences or spread confusion. Developing critical thinking skills, consulting reliable sources, and verifying information before sharing it are essential practices for becoming a responsible and informed digital citizen.

The growing integration of Artificial Intelligence into digital platforms has introduced both new opportunities and new risks. AI technologies increasingly shape the information users receive through personalised recommendations, automated content moderation, targeted advertising, and intelligent search systems. While these technologies can improve efficiency and user experience, they also raise important concerns regarding algorithmic bias, manipulated content, deepfakes, AI-generated misinformation, and reduced transparency in decision-making. Understanding how AI systems operate enables users to recognise potential manipulation, question automated recommendations, and approach digital content with greater awareness and critical judgement.

Other digital risks should not be overlooked. Malicious software, insecure public Wi-Fi networks, fake online profiles, account hacking, excessive screen time, and online exploitation are additional challenges that users may encounter throughout their digital lives. Remaining informed about emerging threats and adopting responsible digital behaviours significantly strengthens personal resilience and reduces vulnerability to cyber risks.

Although it is impossible to eliminate every online risk, the vast majority can be significantly reduced through awareness, digital literacy, responsible online behaviour, and informed decision-making. By understanding the nature of these threats and developing practical strategies to address them, individuals can confidently enjoy the many benefits of the digital world while protecting their privacy, security, and overall well-being.

Awareness is the foundation of digital safety. The more we understand online risks, the better equipped we are to recognise them, respond appropriately, and create a safer digital environment for ourselves and others.

Chapter 3. Cyberbullying, Online Harassment and Digital Abuse

Digital communication has transformed the way people connect, collaborate, and build relationships. Social media platforms, messaging applications, online communities, and other digital technologies allow individuals to communicate instantly, share ideas, and participate in global conversations. While these developments have created significant opportunities for learning, creativity, and social interaction, they have also given rise to new forms of harassment and abuse that can seriously affect an individual's safety, dignity, and overall well-being.

Cyberbullying refers to repeated and intentional behaviour aimed at intimidating, threatening, humiliating, or harming another person through digital technologies. Unlike traditional forms of bullying, cyberbullying can occur at any time, reach large audiences within seconds, and continue beyond physical environments such as schools or workplaces. It may involve insulting or offensive comments, spreading false rumours, sharing private information or images without consent, impersonating another person online, publishing humiliating content, deliberately excluding individuals from online communities, or repeatedly sending threatening or abusive messages. The anonymity provided by some digital platforms can sometimes encourage harmful behaviour, making it more difficult for victims to identify those responsible.

Young women are often disproportionately affected by various forms of online harassment and digital abuse. Appearance-based criticism, body shaming, unwanted messages, gender-based discrimination, sexual harassment, cyberstalking, online intimidation, hate speech, and the non-consensual sharing of personal photographs or videos remain widespread challenges across many digital platforms. These experiences not only violate individuals' privacy and dignity but may also discourage them from participating confidently in online spaces, expressing their opinions, or engaging with digital communities.

The consequences of cyberbullying and online harassment extend far beyond the digital environment. Victims may experience anxiety, stress, depression, loneliness, reduced self-confidence, fear, and emotional exhaustion. In some cases, prolonged exposure to online abuse can negatively affect academic performance, professional development, personal relationships, and overall mental health.

Because digital content can spread rapidly and remain accessible for long periods of time, the emotional impact of online abuse may continue long after the original incident has occurred. Recognising the early signs of cyberbullying is an important step towards protecting yourself and others. Repeated hostile messages, persistent unwanted contact, public humiliation, deliberate exclusion from online groups, or the circulation of harmful or false content should never be dismissed as harmless online behaviour. Every individual has the right to feel safe, respected, and protected while participating in digital environments.

If you experience cyberbullying or online harassment, remember that you are not alone and that support is available. It is advisable to avoid responding impulsively or engaging in further confrontation. Instead, preserve evidence by taking screenshots, saving messages, or recording relevant information before using the reporting mechanisms available on digital platforms.

Blocking abusive users and informing trusted family members, friends, educators, youth workers, or other support services can help prevent further harm and ensure that appropriate assistance is provided. Seeking emotional support is equally important, as talking openly about these experiences can significantly reduce feelings of isolation and distress.

Equally important is becoming an active and responsible digital bystander. If you witness online harassment, avoid encouraging or sharing abusive content, even unintentionally. Instead, where appropriate, offer support to the affected individual, report harmful behaviour through the platform's reporting tools, and promote respectful online communication. Every positive action contributes to creating digital communities based on empathy, inclusion, and mutual respect.

Building safer digital environments is a shared responsibility. By treating others with kindness, respecting diversity, protecting privacy, and challenging harmful online behaviour, we contribute to a culture where everyone can participate confidently and safely in the digital world. Respect, empathy, and responsibility are the foundations of every healthy digital community. Together, we can create online spaces where everyone feels safe, valued, and empowered to participate without fear of harassment or discrimination.

Chapter 4. Protecting Your Privacy and Personal Data

Your personal information is one of your most valuable digital assets. Every time you create an account, share a photograph, make an online purchase, or use a mobile application, you generate personal data that may be collected, analysed, or stored.

Protecting your privacy begins with understanding what information you choose to share. Details such as your full name, address, telephone number, financial information, location, daily routines, photographs, and identification documents should always be shared carefully and only when necessary.

Privacy settings available on social media platforms and digital applications provide valuable tools for controlling who can view your content and access your personal information. Regularly reviewing these settings ensures that your accounts remain aligned with your preferred level of privacy.

Many websites and applications request access to information such as your location, contacts, camera, microphone, or browsing activity. Before granting these permissions, carefully consider whether they are genuinely required for the service you intend to use. Limiting unnecessary permissions significantly reduces potential privacy risks.

It is equally important to remain cautious when using public Wi-Fi networks, downloading unfamiliar applications, or clicking on unknown links. These situations may expose your personal information to cybercriminals or malicious software.

Protecting your personal data is not only about preventing cybercrime, it is about maintaining control over your digital identity, preserving your rights, and ensuring that your online presence reflects your own choices rather than those of others.

Remember that privacy is a fundamental right. Every informed decision you make contributes to a safer, more secure, and more responsible digital experience.

Chapter 5. Creating Strong Passwords and Securing Your Accounts

In today's digital society, our online accounts provide access to personal conversations, financial information, educational resources, healthcare services, social media platforms, and countless other aspects of everyday life. Consequently, protecting these accounts has become an essential part of safeguarding our personal identity and maintaining our digital security.

Passwords represent the first barrier against unauthorised access to our personal information. Weak, predictable, or reused passwords significantly increase the likelihood of cybercriminals gaining access to sensitive data. Once compromised, a single password may expose multiple online accounts, leading to identity theft, financial loss, or misuse of personal information.

A secure password should be long, unique, and difficult to guess. It is advisable to combine uppercase and lowercase letters, numbers, and special characters while avoiding obvious information such as names, birthdays, favourite sports teams, or simple number sequences. Equally important is using a different password for every online account, ensuring that a security breach affecting one platform does not automatically compromise others.

Whenever possible, users should activate Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA). These additional security measures require users to verify their identity through a second authentication step, such as a code sent to a mobile device or generated by an authentication application. Even if a password is stolen, this extra layer of protection greatly reduces the risk of unauthorised access.

Regularly reviewing account activity is another important habit. Many online platforms allow users to view recent login history and identify unfamiliar devices or locations. If suspicious activity is detected, passwords should be changed immediately, active sessions terminated, and additional security settings reviewed.

It is equally important to remain cautious when receiving unexpected emails or messages requesting login credentials. Legitimate organisations rarely ask users to disclose passwords via email or messaging platforms. Such requests often indicate phishing attempts designed to steal personal information.

Good Practices for Strong Account Security

- Create passwords containing at least 12–16 characters.
- Avoid reusing passwords across multiple platforms.
- Enable Multi-Factor Authentication whenever available.
- Never share passwords with others.
- Update passwords if you suspect a security breach.
- Use a trusted password manager to securely store credentials.

Remember

A strong password protects much more than an account—it protects your identity, your privacy, and your digital life.



Chapter 6. Safe Social Media Practices

Social media has transformed the way people communicate, build relationships, access information, and express themselves. Platforms such as Instagram, Facebook, TikTok, Snapchat, LinkedIn, and many others offer valuable opportunities for creativity, networking, education, and community engagement. However, responsible participation in these digital spaces requires awareness, critical thinking, and careful decision-making.

Every post, photograph, comment, reaction, or shared location contributes to what is commonly known as a digital footprint—the permanent record of our online activity. Although certain content may later be deleted, copies, screenshots, or archived versions often remain accessible. For this reason, every online action deserves careful consideration before publication. Users should regularly review the privacy settings available on their social media accounts. Restricting profile visibility, controlling who can view personal information, limiting location sharing, and managing permissions for third-party applications are simple but effective ways to enhance online privacy.

Equally important is exercising caution when interacting with unknown individuals online. Friend requests, direct messages, or invitations from unfamiliar accounts should always be approached carefully, particularly when they involve requests for personal information, photographs, or financial assistance.

Responsible social media use also involves respectful communication. Online interactions should reflect the same values expected in face-to-face conversations, including kindness, empathy, honesty, and respect for diversity. Harassment, discrimination, hate speech, misinformation, and offensive language contribute to unsafe online communities and negatively affect both individuals and society. It is also important to recognise that social media often presents an edited and idealised version of reality.

Images are frequently filtered, achievements selectively presented, and everyday struggles rarely visible. Comparing ourselves with carefully curated online content may negatively influence self-esteem and emotional well-being.

Developing healthy social media habits allows individuals to enjoy the benefits of digital communication while maintaining control over their privacy, reputation, and emotional health.

Questions to Ask Before Posting

Before sharing content online, consider the following:

- Would I be comfortable if this content remained online permanently?
- Could this information be misused?
- Does this post respect my privacy and the privacy of others?
- Am I sharing this for positive reasons?
- Would I feel comfortable if a future employer, teacher, or family member viewed this content?

Key Message

Think before you post, your digital reputation is built one click at a time.



Chapter 7. Artificial Intelligence in Everyday Life

Artificial Intelligence (AI) is no longer a technology of the future—it has become an integral part of our everyday lives. Whether we are searching the internet, watching videos, shopping online, navigating through cities, translating languages, or using social media platforms, Artificial Intelligence quietly supports many of the digital services we rely upon every day.

AI systems are designed to analyse large amounts of information, recognise patterns, automate repetitive tasks, and generate recommendations that personalise our digital experiences. This enables technology to respond more efficiently to users' preferences and behaviours, often improving convenience, accessibility, and productivity.

For example, streaming platforms recommend films and music based on previous viewing habits, online shops suggest products related to earlier purchases, navigation systems identify the fastest travel routes, while social media platforms prioritise content they predict users will find interesting.

Although these personalised experiences can be extremely useful, they also influence the information we consume and the choices we make. Recommendation algorithms may gradually limit exposure to diverse viewpoints by repeatedly presenting similar content. This phenomenon, often referred to as a filter bubble, may affect our understanding of current events, opinions, and social issues.

Artificial Intelligence is also increasingly used in education, healthcare, banking, public administration, scientific research, and environmental protection. These applications demonstrate AI's enormous potential to improve quality of life while addressing complex societal challenges.

Understanding how AI operates allows individuals to become active rather than passive users of technology. Digital literacy today includes recognising when Artificial Intelligence is influencing online experiences and developing the ability to critically evaluate automated recommendations instead of accepting them unquestioningly.

Examples of AI in Everyday Life

Artificial Intelligence is present whenever you:

- receive personalised recommendations on Netflix or Spotify;
- use voice assistants such as Siri or Google Assistant;
- translate text automatically;
- unlock your smartphone using facial recognition;
- receive personalised advertisements online;
- navigate using GPS applications;
- interact with customer-service chatbots.

Key Message

Artificial Intelligence is a powerful tool. Understanding how it works empowers you to use it responsibly rather than allowing it to shape your decisions without awareness.



Chapter 8. Ethical AI: Opportunities, Risks and Bias

Artificial Intelligence offers extraordinary opportunities for innovation and social progress. It has the potential to improve healthcare, support scientific discoveries, optimise public services, facilitate communication, enhance accessibility for people with disabilities, and contribute to more sustainable societies.

However, every technological innovation also carries responsibilities. Artificial Intelligence systems are designed and trained by humans using historical data. Consequently, AI may unintentionally reproduce existing social inequalities, stereotypes, or discrimination present within those datasets.

Algorithmic bias occurs when AI systems produce unfair or inaccurate outcomes that disadvantage particular individuals or groups. Such bias may influence employment recruitment, financial services, educational opportunities, healthcare recommendations, and criminal justice systems. Understanding these limitations is essential for promoting fairness and accountability.

Another growing concern involves deepfake technologies and AI-generated content. Advances in generative AI now make it possible to create highly realistic images, videos, and voices that appear authentic despite being entirely fabricated. These technologies can be used creatively, but they may also contribute to misinformation, identity fraud, and reputational harm.

Ethical Artificial Intelligence is guided by several fundamental principles, including transparency, fairness, accountability, privacy, inclusiveness, human oversight, and respect for human rights. Responsible AI development seeks to ensure that technological innovation benefits society while minimising potential harms.

As digital citizens, we also share responsibility for using AI ethically. This includes verifying AI-generated information, respecting intellectual property, avoiding misuse of AI tools, protecting personal data, and remaining aware that AI-generated responses are not always accurate or unbiased.

Developing ethical awareness enables us to become informed users who appreciate the opportunities offered by Artificial Intelligence while recognising its limitations and potential risks.

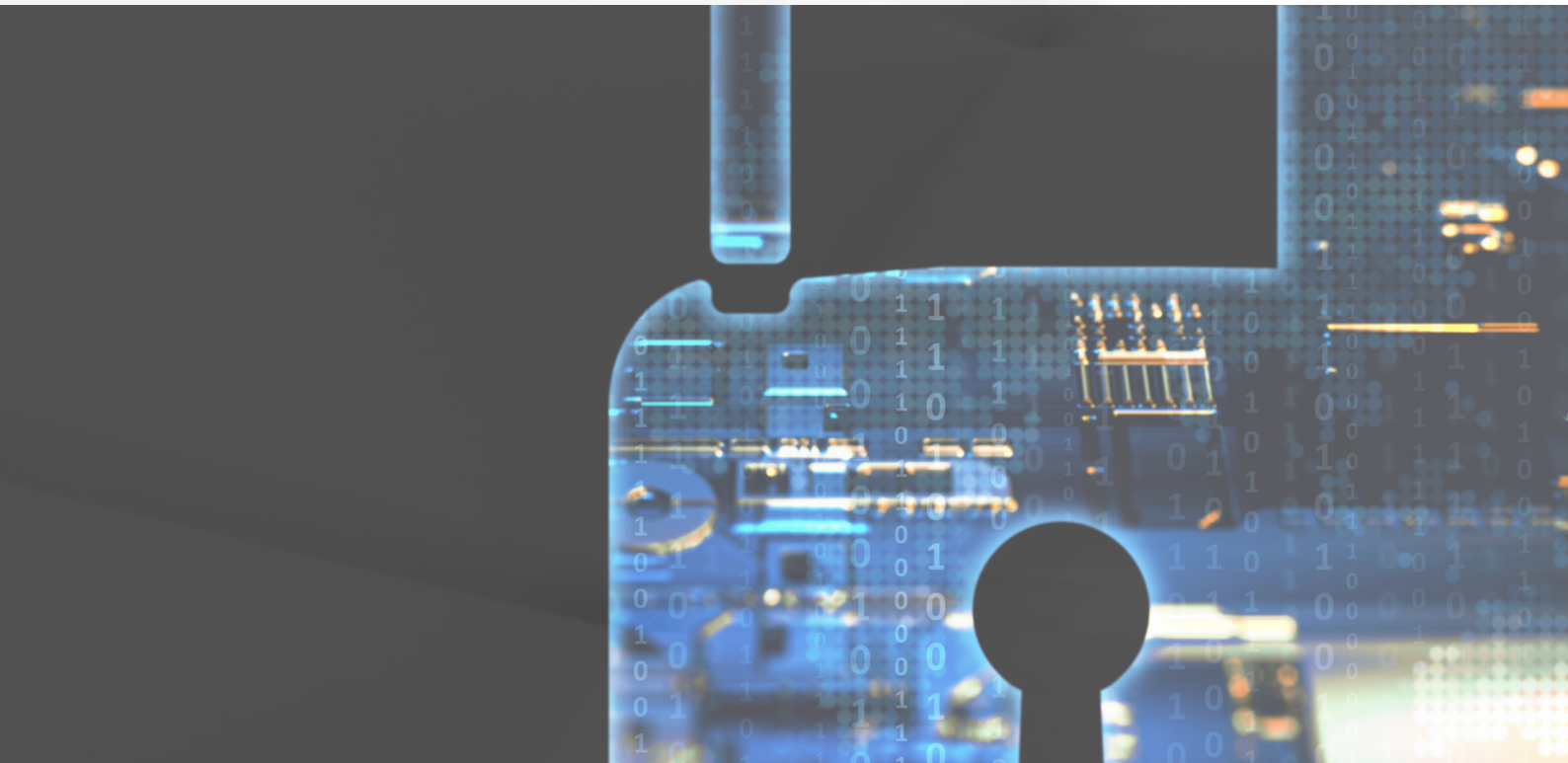
Responsible AI Principles

Ethical AI should always be:

- Transparent
- Fair
- Inclusive
- Accountable
- Secure
- Respectful of privacy
- Human-centred

Key Message

Artificial Intelligence should always serve people, not replace human judgement, responsibility, or ethical decision-making.



Chapter 9. Digital Well-being and Mental Health

Digital technologies have become deeply integrated into our daily routines. They enable us to stay connected with friends and family, access educational resources, express creativity, and participate in communities across the world. When used consciously, technology enriches our lives and expands opportunities for learning and collaboration.

However, excessive or unbalanced digital engagement may also influence our emotional health and psychological well-being. Constant notifications, prolonged screen time, social comparison, online pressure, cyberbullying, and continuous exposure to digital content may contribute to stress, anxiety, sleep disturbances, reduced concentration, and lower self-esteem.

Digital well-being refers to maintaining a healthy, balanced, and positive relationship with technology. Rather than avoiding digital tools, digital well-being encourages individuals to use them intentionally, ensuring that technology supports personal development without negatively affecting physical or emotional health. Developing healthy digital habits begins with becoming aware of our own patterns of technology use. Taking regular breaks from screens, establishing device-free moments during the day, prioritising face-to-face interactions, engaging in physical activity, and dedicating time to hobbies all contribute to greater emotional resilience and improved mental health.

Equally important is recognising emotional warning signs. If online activity consistently generates feelings of stress, sadness, isolation, or anxiety, it may be time to reassess digital habits and seek support from trusted friends, family members, educators, youth workers, or mental health professionals. Technology should empower us to connect, learn, and grow—not overwhelm us or determine our self-worth.

Healthy Digital Habits

- Set daily screen-time boundaries.
- Take regular breaks from digital devices.
- Avoid using screens immediately before bedtime.
- Spend time outdoors and remain physically active.
- Follow content that inspires and educates.
- Unfollow accounts that negatively affect your well-being.
- Prioritise meaningful offline relationships.

Remember

Your mental health is more important than your notifications. A healthy digital life begins with conscious choices, balanced habits, and self-care.

Chapter 10. Building Healthy Digital Habits

Technology has become an essential part of modern life, providing unprecedented opportunities for learning, communication, creativity, and personal development. However, developing a healthy relationship with digital technologies requires conscious choices and balanced habits that support both productivity and personal well-being.

Healthy digital habits are not about avoiding technology altogether; rather, they involve using digital tools intentionally, responsibly, and in ways that enhance rather than diminish our quality of life. By becoming more aware of how we interact with digital devices, we can reduce unnecessary stress, improve concentration, strengthen relationships, and protect our mental and emotional health.

One of the most effective strategies is to establish clear boundaries between online and offline activities. Allocating dedicated time for work, study, recreation, and rest helps prevent excessive screen time and promotes a healthier daily routine. Similarly, taking regular breaks from digital devices throughout the day allows both the mind and body to recover from continuous digital stimulation.

Developing healthy habits also includes critically evaluating the content we consume. Following reliable information sources, engaging with positive and educational content, and limiting exposure to harmful or misleading information contribute to a more constructive digital experience. At the same time, reducing interactions with accounts or platforms that generate stress, negativity, or unrealistic comparisons can significantly improve emotional well-being.

Digital habits should also support meaningful human relationships. Although technology facilitates communication across distances, it should never replace genuine face-to-face interactions with family, friends, and local communities. Prioritising real-life conversations, outdoor activities, hobbies, and personal interests helps maintain a healthy balance between digital engagement and everyday life.

Creating healthy digital routines is an ongoing process that requires reflection and self-awareness. Small daily actions, such as silencing unnecessary notifications, scheduling device-free moments, or practising mindful technology use, can lead to significant long-term improvements in overall well-being.

Healthy Digital Habits to Practise Every Day

- Set realistic limits for daily screen time.
- Schedule regular breaks during prolonged device use.
- Create technology-free moments during meals and before bedtime.
- Prioritise meaningful offline relationships and activities.
- Follow reliable and positive online content.
- Regularly review your digital habits and adjust them when necessary.
- Remember that your well-being should always take priority over digital engagement.

Technology should complement your life, not consume it. Healthy digital habits begin with conscious choices made every day.



Chapter 11. Responding to Online Risks and Seeking Support

Despite adopting safe online practices, every internet user may encounter situations that compromise their security, privacy, or emotional well-being. Online risks can take many forms, including cyberbullying, identity theft, online harassment, phishing attempts, privacy breaches, misinformation, or other forms of digital abuse. While these experiences can be distressing, responding appropriately and seeking timely support can significantly reduce their impact.

The first and most important step when confronted with an online threat is to remain calm. Acting impulsively or responding emotionally may unintentionally escalate the situation or expose additional personal information. Taking a moment to assess the circumstances allows individuals to make informed decisions and choose the most appropriate course of action.

Whenever inappropriate or abusive behaviour occurs online, it is advisable to preserve all available evidence before taking further action. Saving screenshots, recording usernames, storing messages, or documenting relevant interactions can prove valuable should the situation require reporting to the platform, educational institutions, employers, or, where necessary, the relevant authorities.

Most social media platforms and digital services provide dedicated reporting mechanisms that enable users to report abusive content, fake accounts, harassment, or violations of community standards. Making use of these reporting tools contributes not only to individual safety but also to creating safer digital environments for all users.

Protecting compromised accounts is equally important. If there is any indication that login credentials or personal information have been exposed, passwords should be changed immediately, Multi-Factor Authentication should be activated where available, and any suspicious account activity should be carefully reviewed. In situations involving financial information or identity theft, contacting the relevant service providers without delay is essential.

Online incidents may also have a profound emotional impact. Feelings of anxiety, embarrassment, fear, frustration, or sadness are natural reactions to experiences such as cyberbullying or digital harassment. Seeking support from trusted family members, friends, educators, youth workers, counsellors, or mental health professionals should never be viewed as a sign of weakness. On the contrary, reaching out for support demonstrates resilience, self-awareness, and a commitment to personal well-being.

It is equally important to remember that every individual has a role in creating safer online communities. Offering support to others, reporting abusive behaviour when witnessed, and promoting respectful communication contribute to digital environments where everyone feels valued, respected, and protected.

Ultimately, responding effectively to online risks requires knowledge, confidence, and the understanding that help is always available. No one should ever feel isolated when facing challenges in the digital world. Digital safety is strengthened when we respond thoughtfully, seek support when needed, and stand together against online abuse and harmful behaviour.



Chapter 12. Useful Digital Safety Tools and Resources

Digital safety extends beyond individual awareness and responsible behaviour. It is also supported by a wide range of technological tools, educational resources, and trusted organisations that help users protect their privacy, strengthen cybersecurity, verify online information, and develop their digital competences.

Modern digital platforms increasingly provide integrated security features designed to protect users from unauthorised access and online threats. Features such as Multi-Factor Authentication, account recovery options, login notifications, privacy controls, and security check-ups allow individuals to better manage their digital identities and reduce potential vulnerabilities. Becoming familiar with these settings and reviewing them regularly represents an important aspect of responsible digital citizenship.

Equally valuable are password management applications, which enable users to generate and securely store complex passwords without relying on memory alone. By encouraging the use of unique passwords across different platforms, these tools significantly reduce the likelihood of multiple accounts being compromised following a single security breach.

As misinformation and AI-generated content become increasingly widespread, fact-checking services and trusted news organisations play an essential role in supporting informed decision-making. Consulting reliable sources before sharing information helps prevent the spread of false or misleading content and contributes to healthier online communities.

Educational resources also represent an important pillar of digital safety. Numerous European initiatives, educational institutions, youth organisations, and online learning platforms provide practical guidance on internet safety, digital literacy, Artificial Intelligence, cybersecurity, and online well-being. Continuous learning allows individuals to remain informed about emerging technologies while adapting to new digital challenges throughout their lives.

Finally, digital safety should always be understood as a shared responsibility. Technology companies, educational institutions, policymakers, youth organisations, families, and individual users all contribute to creating digital environments that are secure, inclusive, and respectful. By making use of available resources and remaining committed to lifelong learning, every individual can strengthen their digital resilience and confidently navigate an increasingly technology-driven world.

Knowledge is one of the most effective tools for digital protection. The more informed we become, the safer and more confidently we are able to participate in the digital world.

Digital Safety Checklist

Developing digital safety is an ongoing process rather than a single achievement. Every online interaction provides an opportunity to make informed decisions that protect personal information, strengthen security, and promote responsible digital behaviour. Reflecting regularly on our own digital practices enables us to recognise both our strengths and the areas where further improvement may be beneficial.

Consider whether your online accounts are protected by strong and unique passwords and whether additional security measures, such as Multi-Factor Authentication, have been activated wherever possible. Reflect on how frequently you review the privacy settings of your social media platforms and digital applications, ensuring that personal information is shared only with those you trust.

Think about the information you publish online and whether you carefully evaluate its potential long-term consequences before sharing it. Consider whether you critically assess digital content, verify information before redistributing it, and remain aware of the ways in which Artificial Intelligence may influence the information presented to you.

It is equally important to reflect upon your emotional relationship with technology. Ask yourself whether your digital habits contribute positively to your well-being or whether adjustments may be needed to establish a healthier balance between online and offline life. Recognising the importance of regular breaks, meaningful face-to-face interactions, physical activity, and time away from screens contributes significantly to maintaining emotional resilience.

Finally, consider whether you know where to seek assistance should you encounter online harassment, privacy violations, misinformation, or other digital risks. Being aware of available support networks is an important component of personal digital preparedness.

Digital safety is not measured by perfection but by continuous learning and conscious improvement. Every positive decision strengthens not only your own security but also contributes to creating a more respectful, inclusive, and trustworthy digital environment for everyone. Every thoughtful digital decision contributes to a safer online experience, for yourself, for your community, and for future generations of digital citizens

Final Thoughts: Becoming a Responsible Digital Citizen

The digital world continues to evolve at an extraordinary pace, creating new opportunities for innovation, communication, education, creativity, and international collaboration. As digital technologies and Artificial Intelligence become increasingly integrated into our everyday lives, the responsibility of using them wisely, ethically, and respectfully becomes equally important.

Being a responsible digital citizen extends far beyond possessing technical knowledge or knowing how to operate digital devices. It involves understanding the broader social, ethical, and human dimensions of technology. Responsible digital citizens communicate respectfully, protect their privacy and the privacy of others, critically evaluate information before accepting or sharing it, and actively contribute to creating digital environments founded on inclusion, empathy, integrity, and mutual respect.

Every interaction in the digital world has consequences. A comment can encourage or discourage another person. A shared photograph can inspire or violate someone's privacy. A piece of information can educate or mislead. Every choice we make online contributes to shaping the quality of our digital communities. Recognising this responsibility allows us to become active participants in building a safer and more ethical digital society.

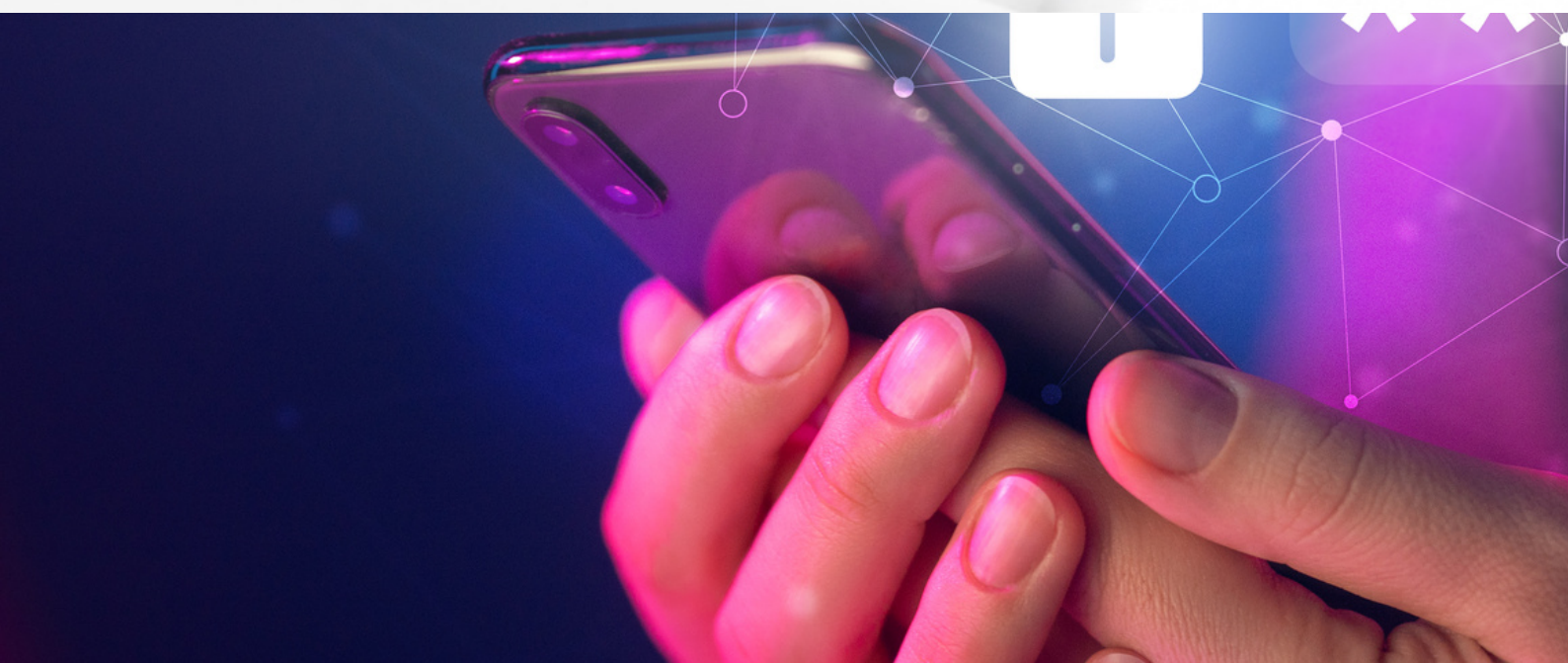
Artificial Intelligence and emerging technologies will continue to influence the future of education, employment, healthcare, communication, and countless other aspects of society. Remaining curious, informed, and committed to lifelong learning will enable us to adapt confidently to these developments while maintaining our ability to make independent, ethical, and well-informed decisions.

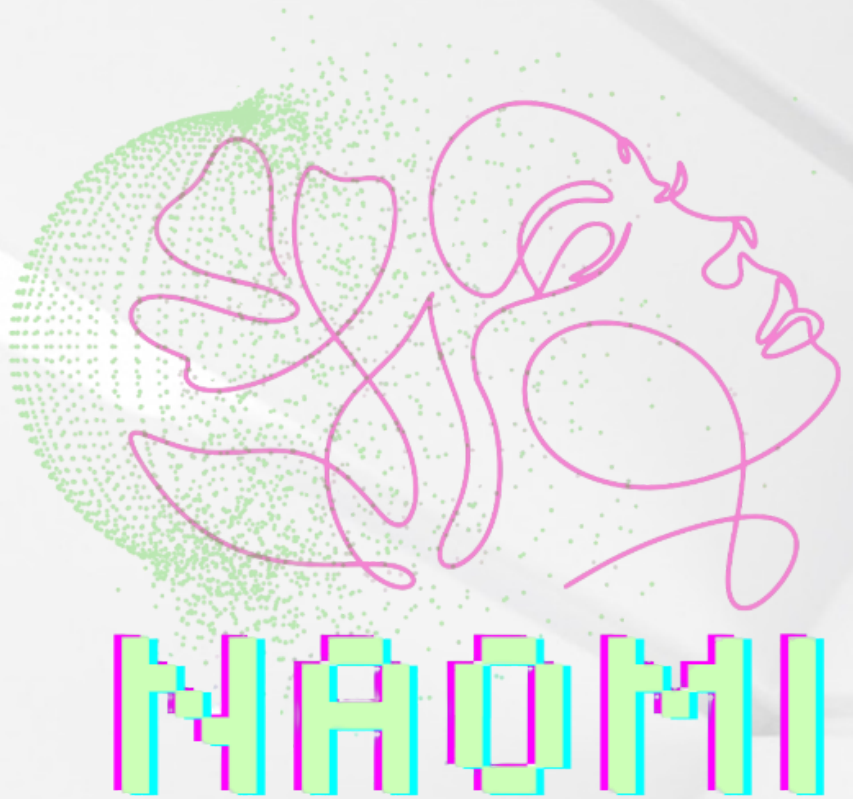
The NAOMI Project believes that every young woman has the capacity to become a confident, informed, and resilient digital citizen. By strengthening digital literacy, promoting responsible Artificial Intelligence, protecting mental well-being, and encouraging ethical online behaviour, we can collectively contribute to a future where technology serves humanity in ways that are fair, inclusive, and empowering.

Digital citizenship is ultimately built through everyday actions. Every responsible decision, every respectful interaction, every effort to verify information, and every commitment to protecting personal well-being contributes to a digital environment where innovation and human values coexist harmoniously.

May this guide serve not only as a practical resource but also as an invitation to continue learning, reflecting, and embracing technology with confidence, responsibility, and integrity.

The future of the digital world depends on the choices we make today. Let those choices be guided by knowledge, responsibility, empathy, and respect, creating a digital society where everyone can learn, connect, and thrive safely.





Navigating AI and Internet Safety for Young Females & Mental Health – NAOMI

Digital Safety Guide

Project Number: 2024-3-FR02-KA210-YOU-000277850

www.naomi-project.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 Agence du Service Civique / Agence Erasmus + France Jeunesse & Sport. Neither the European Union nor the granting authority can be held responsible for them.