



**DEVELOPMENT OF THE
DIGITAL SOVEREIGNTY
COMPETENCES OF YOUTH
WORKERS**

**MANUAL FOR
YOUTH WORKERS**



Co-funded by
the European Union

This content has been prepared within LINKS project No.2021-2-DK01-KA220-YOU-000050308, financed under the Erasmus+ programme. The content of this publication is the sole responsibility of the project coordinator and may not always reflect the views of the European Commission or the National Agency.



This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>



TABLE OF CONTENTS

1.Introduction.....	1
1.1 Understanding the Digital Landscape.....	1
1.2 Importance for Youth Workers.....	2
2. Protecting Devices.....	3
2.1 Safe Internet Practices.....	3
3. Competences for Protecting Personal Data and Privacy.....	5
3.1 Importance of Data Protection as youth workers.....	9
3.2 Rules for online safety.....	13
3.3 Critical evaluation of digital technologies.....	17
4. Protecting Health and Well-Being.....	20
4.1 Health data protection.....	20
4.2 Balancing digital engagement.....	22
5. Protecting the Environment	27
5.1 Environmental impact of digital activities.....	27
5.2 Sustainable Digital Practices.....	30
6. Educational Strategies for Youth Workers.....	32
7. Resources and Tools for Youth Workers:.....	36
8.Conclusion.....	40

1.Introduction

1.1 Understanding the Digital Landscape

In today's technologically driven society, youth workers often rely on digital tools and platforms to engage with and support young people. This entails collecting, storing, and processing sensitive information, ranging from personal details to emotional well-being. It is crucial for youth workers to comprehend the intricacies of data protection laws and regulations to ensure the confidentiality and privacy of the youth they serve. With the ever-evolving digital landscape, staying informed about the latest advancements, cyber threats, and changes in legislation becomes essential. Youth workers must be adept at employing secure communication channels, implementing robust encryption measures, and staying vigilant against potential data breaches to safeguard the trust and welfare of the young individuals they work with.

Moreover, the digital landscape poses challenges and opens up new avenues for effective youth work. Embracing technology allows youth workers to reach a broader audience, offer innovative programs, and gather valuable insights through data analysis. However, striking the right balance between leveraging digital tools for enhanced services and respecting privacy rights is key. Youth workers should undergo continuous training to stay abreast of digital trends, fostering a culture of responsible data management within their organisations. By cultivating a comprehensive understanding of the digital landscape and its implications for data protection, youth workers can optimise their practices, ensuring that their efforts to support and empower young people are effective and ethically sound in the digital age.

1.2 Importance for Youth Workers

Recognising the critical importance of equipping youth workers with the knowledge and skills to navigate online data protection, we have developed a comprehensive manual tailored specifically to their needs. This manual incorporates a unique approach by utilising "digital nuggets" — bite-sized, easily digestible pieces of information strategically designed to convey key concepts and best practices in online data protection. In an era where attention spans are often limited, digital nuggets effectively deliver information without overwhelming the learner. These concise yet informative modules cover topics such as secure data handling, encryption protocols, and ethical considerations when engaging with young people online.

The decision to employ digital nuggets as a training methodology is grounded in the understanding that traditional training methods may fall short in addressing the dynamic nature of the digital landscape. By adopting a more agile and interactive approach, youth workers can absorb relevant information at their own pace, fostering a deeper understanding of the nuances of online data protection. The manual imparts theoretical knowledge and incorporates practical scenarios and case studies, allowing youth workers to apply their learning in real-world contexts. This innovative training approach aims to empower youth workers to confidently navigate the digital sphere, ensuring that they can harness the benefits of technology while upholding the highest standards of data protection for the youth they serve.



2. Protecting Devices

The internet is an invaluable resource for youth workers, offering a vast array of tools and information to aid in their work with young people. However, the digital landscape is also fraught with risks such as cyberbullying, misinformation, privacy breaches, and online predators. Understanding and implementing safe internet practices is crucial for youth workers to protect themselves and the young people they guide. This topic explores essential safe internet practices and how they can be integrated into everyday digital interactions.

2.1 Safe Internet Practices

Key Areas of Focus:

1. **Recognizing and Avoiding Online Threats:** Educate youth workers on identifying common online threats, including cyberbullying, phishing scams, and malware. Understanding these threats is the first step in practicing safe internet habits.
2. **Managing Digital Footprints:** Discuss the importance of being mindful of one's digital footprint. Encourage practices such as thoughtful posting, understanding privacy settings on social media, and the implications of sharing personal information online.
3. **Safe Social Media Usage:** Provide guidelines for safe and responsible use of social media platforms. This includes understanding privacy settings, recognizing the signs of harmful content, and reporting inappropriate or abusive behavior.
4. **Protecting Personal Information:** Emphasize the importance of safeguarding personal and professional information online. This includes not sharing sensitive information like addresses, phone numbers, and financial details on unsecured websites or with unknown entities.
5. **Critical Evaluation of Online Content:** Teach youth workers how to critically assess the reliability and credibility of online information. This skill is vital in an age of widespread misinformation and 'fake news'.

6. **Encouraging Healthy Online Habits:** Discuss the importance of balancing online and offline activities, and the impact of excessive screen time on mental and physical health.

7. **Responding to Cyberbullying and Harassment:** Equip youth workers with strategies to deal with cyberbullying and online harassment, both for themselves and the young people they work with.

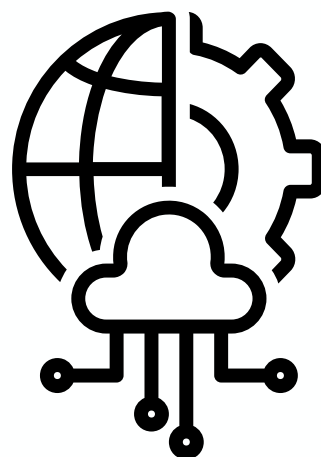
8. **Promoting a Positive Online Environment:** Encourage youth workers to lead by example and foster a positive, respectful online environment. This includes engaging in constructive conversations, respecting differing opinions, and avoiding toxic online behavior.

Conclusion:

Safe internet practices are essential for youth workers, not just for their personal and professional protection but also as a model for responsible digital behavior to the youth they mentor. By adopting and teaching these practices, youth workers can create a safer, more positive online community for themselves and the young people they influence.

Call to Action:

Urge youth workers to continuously educate themselves on safe internet practices and to actively incorporate these lessons into their interactions with young people. Promoting digital literacy and responsible online behavior is a collective effort, essential in cultivating a secure and positive digital future.



3. Competences for Protecting Personal Data and Privacy

Youth workers play a crucial role in guiding and supporting young individuals in today's digital age, making it imperative for them to possess a deep understanding of how the internet works, the dynamics of online marketing, and other digital competencies outlined in frameworks like DigComp.

The DigComp framework identifies the key components of digital competence in 5 areas (Dimension 1). The areas are summarised below:
Information and data literacy: To articulate information needs, to locate and retrieve digital data, information and content. To judge the relevance of the source and its content. To store, manage, and organise digital data, information and content.

Communication and collaboration: To interact, communicate and collaborate through digital technologies while being aware of cultural and generational diversity. To participate in society through public and private digital services and participatory citizenship. To manage one's digital presence, identity and reputation.

Digital content creation: To create and edit digital content To improve and integrate information and content into an existing body of knowledge while understanding how copyright and licences are to be applied. To know how to give understandable instructions for a computer system.

Safety: To protect devices, content, personal data and privacy in digital environments. To protect physical and psychological health, and to be aware of digital technologies for social well-being and social inclusion. To be aware of the environmental impact of digital technologies and their use.

Problem solving: To identify needs and problems, and to resolve conceptual problems and problem situations in digital environments. To use digital tools to innovate processes and products. To keep up-to-date with the digital evolution.

Understanding how the internet works is fundamental for youth workers to navigate the vast online world effectively. This includes knowledge about internet infrastructure, protocols, and the ability to guide young people in using online resources responsibly. Digital literacy is a key component of youth work in the modern era.

Additionally, youth workers need insights into how online marketing works to help young individuals navigate the digital marketplace. Understanding targeted advertising, data privacy implications, and the influence of online promotions is crucial in guiding informed and responsible consumer behaviour. Proficiency in digital communication tools and strategies enables youth workers to connect more effectively with young individuals.

Lastly, with cyber threats becoming more prevalent, youth workers must comprehend the intricacies of online security. This involves recognising potential risks, teaching safe online practices, and instilling an understanding of cybersecurity measures to protect both personal and professional information.

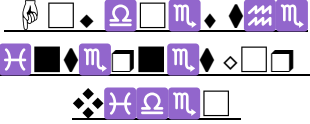
In this unit, we provide a lesson plan to equip youth workers with a solid understanding of how the internet functions, digital marketing dynamics, and competencies outlined in frameworks like DigComp are better positioned to empower and guide young individuals in the digital realm. These competencies not only enhance the quality of youth work but also contribute to the holistic development of digitally literate and responsible citizens.





LESSON PLAN

TOPIC: COMPETENCES FOR PROTECTING PERSONAL DATA AND PRIVACY

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Workshop Opening:</p> <ul style="list-style-type: none"> • Introduction • DigComp Summary • Describe the Lesson Plan and Learning Outcomes 	10 minutes	<p>Training venue with IT equipment. Projector and screen. Laptop.</p> <p>Manual-Digital Sovereignty Competences for Youth Workers Unit 3.0</p> <p>Competences for Protecting Personal Data and Privacy</p>	<p><i>Learners will understand the overall importance of digital competences as youth workers</i></p>
<p>Activity 1: How does the internet work?</p> <ul style="list-style-type: none"> • TCP/ICP • DNS • Routers • Servers 	15 minutes	<p><u>Links online platform</u> Digital Sovereignty Competences training course</p> <p><u>Unit 3. Competences for Protecting Personal Data and Privacy.</u></p> 	<p><i>Learners will understand how the internet works, is accessed and used</i></p>
<p>Activity 2: How does online marketing work?</p> <ul style="list-style-type: none"> • Ads • Personalisation • Online shopping scams 	15 minutes	<p><u>Links online platform</u> Digital Sovereignty Competences training course</p> <p><u>Unit 3. Competences for Protecting Personal Data and Privacy.</u></p> <p><u>Online Marketing Prezi</u></p>	<p><i>Learners will learn how online marketing works and targets consumers</i></p>



LESSON PLAN

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Activity 3: Reflection</p> <p>Ask participants to reflect own experiences and knowledge using guided questions</p> <ul style="list-style-type: none">• What areas of digital literacy do you struggle with?• What risks come with internet access and online marketing?	10 minutes	Paper and pen for individual reflections Whiteboard or poster paper to share answers	<i>Learners will internalise and apply the lessons to their own workplaces</i>

3.1 Importance of Data Protection as youth workers

The digital world has become an integral space for communication, education, and engagement for youth workers. However, it can also introduce serious risks and dangers, especially when dealing with sensitive data and privacy issues surrounding youth.

In this unit, we explore the importance of data protection. The **General Data Protection Regulation** (GDPR) is a comprehensive set of data protection rules established by the European Union (EU) to safeguard the privacy and personal data of individuals.

While your organisation must have an overall GDPR policy that covers all the required principles, as youth workers, it's important that you are aware of these key principles:

1. Purpose Limitation: Personal data should be collected for specified, explicit, and legitimate purposes and should not be further processed in a manner incompatible with those purposes.
2. Data Minimisation: Only the necessary and relevant personal data for the intended purposes should be processed and organisations should avoid collecting excessive or irrelevant information.
3. Integrity and Confidentiality (Security): Organisations must implement appropriate technical and organisational measures to ensure the security of personal data. Protection against unauthorised or unlawful processing, accidental loss, destruction, or damage is essential.

Given the nature of their work, youth workers often handle sensitive **personal data**, including medical information, emergency contacts, and health records. When collecting data about the young people, it's important to only collect essential data for specific purposes. For example, when organising an online workshop, you may collect names and emails but you probably don't need to collect addresses and gender.



The need for youth workers to possess essential digital and cybersecurity skills is paramount to protect youth and their data. Cybersecurity safeguards data, devices, and networks from attackers and potential harm. This involves device security, whether one connects through a computer, laptop, smartphone, or tablet. If your organisation provides a work phone or laptop, it's important to avoid using personal devices when working. Similarly, avoid public wifi networks and use a strong unique password on any device that has personal data.

Youth workers must also be equipped to avoid common online attacks such as password attacks, phishing, identity theft, scams, and malware. Be sure to avoid clicking links in emails with unknown senders or giving personal information out online unless you've verified the sender.

As a youth worker, you should be skilled in these competences to protect the personal data you work with as well as teach youth how to defend their own personal data and uphold their online privacy as well.

In this unit, we provide a lesson plan to facilitate youth workers understanding essential knowledge related to the rules of online safety. By incorporating discussions on privacy, intellectual property rights, steps to stay safe online, and technological literacy, this unit aims to equip youth workers with the tools they need to navigate the digital realm responsibly and educate the next generation on the importance of safeguarding their online presence.



LESSON PLAN

TOPIC: IMPORTANCE OF DATA PROTECTION AS YOUTH WORKERS

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Workshop Opening:</p> <ul style="list-style-type: none"> • Introduction • GDPR Summary • Describe the Lesson Plan and Learning Outcomes 	5 minute	<p>Training venue with IT equipment. Projector and screen. Laptop.</p> <p>Manual-Digital Sovereignty Competences for Youth Workers Unit 3.1</p> <p>Importance of Data Protection as Youth Workers</p>	<p><i>Learners will understand the overall importance of data protection as youth workers</i></p>
<p>Activity 1: Privacy and Intellectual Property</p> <ul style="list-style-type: none"> • What are common privacy and copyright laws? • What defines a trademark? • How does fair use work? 	15 minutes	<p><u>Links online platform</u> Digital Sovereignty Competences training course</p> <p><u>Unit 2.Competences for Protecting Personal Data and Privacy.</u></p> <p><u>Privacy and intellectual property infographic</u></p>	<p><i>Learners will understand the difference between privacy and copyright laws as well as rules surrounding trademarks and fair use</i></p>



LESSON PLAN

TOPIC: IMPORTANCE OF DATA PROTECTION AS YOUTH WORKERS

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Activity 2: How to Implement Security Measures</p> <ul style="list-style-type: none"> • Define 2FA, encryption, firewall, VPN • Teach secure habits such as choosing strong passwords and avoiding phishing attacks 	15 minutes	<p>Links online platform Digital Sovereignty Competences training course</p> <p>Unit 2.Competences for Protecting Personal Data and Privacy</p> <p>How to Implement Security Measures Quiz</p>	<p><i>Learners will learn essential security vocabulary and safety tips</i></p>
<p>Activity 3: Technological Literacy</p> <ul style="list-style-type: none"> • Learn what technological literacy is • Learn how to develop and overcome challenges in improving technological literacy 	15 minutes	<p>Links online platform Digital Sovereignty Competences training course</p> <p>Unit 2.Competences for Protecting Personal Data and Privacy</p> <p>Privacy and intellectual property infographic</p>	<p><i>Learners will understand the difference between privacy and copyright laws as well as rules surrounding trademarks and fair use</i></p>

3.2 Rules for online safety

When we address the concept of online safety, we are referring to the act of staying safe online, which means being able to recognize and avoid exposure to the multiple risks that can be encountered online whenever a person connects to any technological device who has access to the network. Internet, PC, laptop, smartphone and tablet etc. Online security is also commonly known as Internet security, electronic security and computer security.

To do this it is necessary Youth Workers need to possess the digital skills that allow them to navigate safely the vast online world; for this purpose, the DigiComp 2.2 framework was created and comes in handy.

Digital skills are a set of knowledge, skills and competences about knowing how to manage information, social relationships and content by making the best use of the tools and technologies.

In this landscape, the aspects of digital sovereignty and data protection/privacy become even more important for youth workers. Due to the very nature of their work, youth workers have access to and/or process sensitive personal data and information such as medical details, names of emergency contacts, health administration numbers, etc.

It becomes of utmost importance for Youth Workers to recognize how to be safe online and protected from online harms and risks that can violate personal information, privacy, lead to unsafe communications or even compromise mental health and well-being.

Cybersecurity protects data, devices, and networks from attackers, criminals, and anyone who harms a system. Any software that contains sensitive information, such as medical records or financial information, must be equipped to handle cyber-attacks to prevent theft or corruption. Taking inadequate security measures could expose your devices and data to malicious threats such as malicious software. Some of the most common cyber threats can be Password attacks, Phishing and identity theft, Grooming, Scams, Malware.

.

Therefore, for youth workers, the ability to manage data efficiently and securely online is essential. To do this it is necessary to possess adequate digital skills and know cybersecurity measures to be able to transmit to students the knowledge necessary to defend their personal data and online privacy.

In this unit we propose an example of a lesson plan to facilitate Youth Workers in transmitting knowledge relating to the rules for online safety





LESSON PLAN

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Workshop Opening:</p> <ul style="list-style-type: none"> The facilitator opens the workshop by welcoming all learners and briefly introducing the topic of online safety, explaining why it is important to address it 	5 minutes	<p>Training venue with IT equipment. Projector and screen. Laptop.</p> <p>Manual-Digital Sovereignty Competences for Youth Workers Unit 3.2 Rules for online safety.</p>	Learners will gain an overview of what digital skills are, why they are important and they will be able to deepen the knowledge of the DigiComp Framework tool.
<p>Activity 1: Digital skills through the DigiComp framework</p> <ul style="list-style-type: none"> What are Digital Skills How to develop them How to use the DigiComp 	15 minutes	<p><u>Links online platform</u> Digital Sovereignty Competences training course Unit <u>2.Competences for Protecting Personal Data and Privacy</u> <u>Video</u> <u>Digital Skills</u></p> <p><u>DigiComp 2.2 Framework</u></p>	Learners will gain an overview of what digital skills are, why they are important and they will be able to deepen the knowledge of the DigiComp Framework tool.
<p>Activity 2: Online safety rules</p> <ul style="list-style-type: none"> What is cybersecurity Digital sovereignty and privacy protection 	15 minutes	<p><u>Links online platform</u> Digital Sovereignty Competences training course Unit <u>2.Competences for Protecting Personal Data and Privacy</u> Infographic <u>Rules for online safety</u></p>	Learners will gain an overview of some actions to undertake to maintain a certain level of online security



LESSON PLAN

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<ul style="list-style-type: none"> Activity 3: Reflection 	5 minutes	<p>Based on the topics covered in activities 2 and 3, ask participants to share their knowledge and personal experience in this regard.</p> <p>Guiding questions can be used to facilitate reflection:</p> <p>Have you ever been the victim of a cyber attack?</p> <p>Have you ever experienced dangerous situations online?</p> <p>Reading the DigiComp framework, what skills do you think you need to improve/develop to feel safe online?</p>	Learners will integrate the concept learned within the lesson with their own experience
Workshop Close and Feedback	5 minutes	<u>The facilitator ends the workshop with a short recap of all the findings from activity 3</u>	

3.3 Critical evaluation of digital technologies

A safe use of technology cannot leave behind the development of critical thinking skills, to possess the necessary skills to process information online but also to optimally use digital tools in education and daily life.

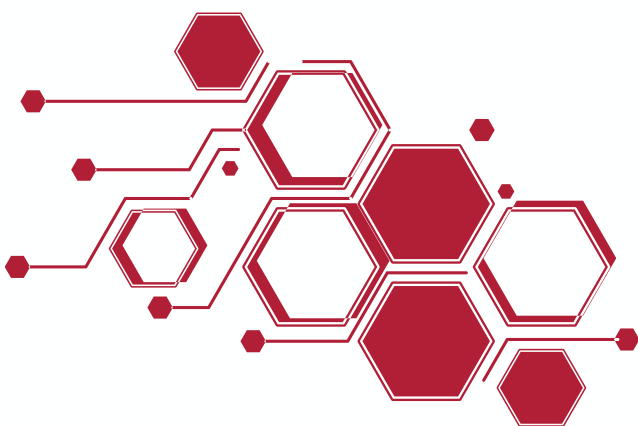
In every area of a person's life in fact, nowadays technology has imposed their presence out of necessity or convenience, we have for example online services for managing issues relating to one's health or finances. With the COVID-19 pandemic, this trend has become increasingly growing given the impossibility created by the situation of physically going to the places where actions previously took place in person, building a network of actions to be carried out remotely online.

In this context, the role of Youth Workers becomes essential to guide learners in a critical and effective but also safe use of technologies.

Critical thinking is the intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing and evaluating information to reach a conclusion.

To remain safe online and for Protecting Personal Data and Privacy using your own digital sovereignty skills, the first step to take is having the ability to critically analyze and evaluate the enormous amount of information we are subjected to, when we are online, but also learn to use the digital tools at our disposal in our daily lives, in a conscious and optimal way to exploit their benefits and minimize the risks.

In this unit we propose an example of a lesson plan to facilitate Youth Workers promoting ways to critically evaluate digital technologies applied to different contexts such as work or education.





LESSON PLAN

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Workshop Opening:</p> <ul style="list-style-type: none"> • Introduction • DigComp Summary • Describe the Lesson Plan and Learning Outcomes 	10 minutes	<p>Training venue with IT equipment. Projector and screen. Laptop.</p> <p>Manual-Digital Sovereignty Competences for Youth Workers Unit 3.0 Competences for Protecting Personal Data and Privacy</p>	<p>Learners will learn through the case study the importance of digital sovereignty in protecting their personal data online, by analyzing the risks that arise if spread without critically analyzing the circumstances</p>
<p>Activity 1: Critically evaluate digital technology</p> <ul style="list-style-type: none"> • Risks of use technologies • “Enjoy cars” case study • Digital sovereignty 	15 minutes	<p><u>Links online platform</u> Digital Sovereignty Competences training course Unit 2.<u>Competences for Protecting Personal Data and Privacy Case study</u></p>	<p>Learners will learn through the case study the importance of digital sovereignty in protecting their personal data online, by analyzing the risks that arise if spread without critically analyzing the circumstances</p>



LESSON PLAN

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Activity 2: Quiz “Use digital technologies in a meaningful way for working and studying”</p> <p>Digital tools applied to work and education</p> <p>Smart use of digital tools</p> <p>Critical use of digital technologies</p>	5 minutes	<p>Links online platform</p> <p>Digital Sovereignty Competences training course Unit 2.Competences for Protecting Personal Data and Privacy</p> <p>Quiz “Use digital technologies in a meaningful way for working and studying”</p>	<p>Learners will gain an overview of some smart ways to use technologies in educational and work environments to maximize their benefits</p>
<p>Activity 3: Quiz “Use digital technologies in a meaningful way for everyday activities”</p> <ul style="list-style-type: none"> Digital tools applied to everyday life Smart use of digital tools Critical use of digital technologies 	5 minutes	<p><u>Links online platform</u></p> <p>Digital Sovereignty Competences training course Unit 2.<u>Competences for Protecting Personal Data and Privacy</u></p> <p><u>Case study</u></p>	<p>Learners will test their abilities to use technologies in a smart ed effective way to facilitate their daily lives</p>

4. Protecting Health and Well being

Data sovereignty refers to the concept that data is subject to the laws and regulations of the country in which it is located. In the context of health data, ensuring data sovereignty is crucial to protect sensitive information and uphold individual privacy. On the other hand, the protection of well-being extends beyond mere compliance to encompass ethical considerations, transparency, and trust-building with individuals. By prioritizing privacy and seeking explicit consent, healthcare entities not only comply with regulations but also contribute to the mental and emotional well-being of individuals.

4.1 Health data protection

Youth workers often handle sensitive health information of young individuals, including medical history, mental health concerns, and other confidential details. Understanding health data protection ensures that youth workers can navigate legal and ethical responsibilities associated with handling such information, preventing unauthorized access or data breaches.

Moreover, as young individuals may be more vulnerable to privacy invasions or misuse of their health data, youth workers play a pivotal role in advocating for and implementing robust security measures. Being knowledgeable about data protection allows youth workers to effectively communicate with young people about the importance of privacy, obtain informed consent, and foster a sense of trust in the healthcare system.

In the context of youth workers' overall well-being, having a solid understanding of health data protection helps mitigate the potential psychological and emotional impact of data-related stressors. It enables youth workers to navigate their responsibilities with confidence, ensuring that they contribute to a supportive and ethical healthcare environment.

Below you will find the lesson outline in order to achieve the gain of knowledge regarding health data protection. By the end of this lesson, youth workers will be able to seamlessly integrate health data protection principles into their everyday practices, ensuring the confidentiality of sensitive information while promoting the well-being of the young individuals they interact with.

Duration	Lesson Outline:
(15 minutes)	Icebreaker Activity -Engage participants with a brief activity to highlight the importance of trust in their relationships with young individuals.
(20 minutes)	Introduction to Health Data Protection - Discuss the key principles of health data protection and their relevance to youth work.
(30 minutes)	Interactive Session: Real-world Examples <ul style="list-style-type: none"> • Present positive examples of organizations or youth workers effectively handling health data. • Facilitate a discussion on why these examples are successful and how they contribute to the overall well-being of young individuals.
(25 minutes)	Group Discussion: Ethical Dilemmas <ul style="list-style-type: none"> • Present ethical dilemmas related to health data in youth work. • Break participants into small groups to discuss and propose solutions that prioritize both data protection and well-being.

4.2 Balancing digital engagement

Introduction:

In today's digital age, the pervasive presence of technology has transformed how we live, work, and interact with the world around us. From social media platforms to streaming services, digital technology offers unprecedented communication, entertainment, and learning opportunities. However, amidst the countless benefits of digital engagement, there lies a pressing need to address the potential risks and challenges it poses to our health and well-being.

Balancing digital engagement is crucial in safeguarding our physical, mental, and emotional well-being in an increasingly digitised world. While technology can connect us with others, facilitate learning, and enhance productivity, excessive or uncontrolled digital usage can harm our health. From digital addiction and sleep disturbances to decreased physical activity and social isolation, the negative impacts of over-engagement with digital devices are well-documented.

Recognising the importance of finding a healthy equilibrium between online and offline activities, balancing digital engagement emphasises the need to establish boundaries, cultivate mindfulness, and prioritise self-care in our digital lives. By striking a balance between the benefits and drawbacks of digital technology, we can mitigate the risks associated with excessive screen time and harness its potential to enrich our lives meaningfully.

In this context, balancing digital engagement becomes paramount in safeguarding our health and well-being. Through awareness, education, and intentional practices, we can empower ourselves to make informed choices about digital usage, prioritise meaningful interactions, and cultivate a healthier relationship with technology. This unit explores the significance of balancing digital engagement and offers practical strategies to promote well-being in an increasingly digitalised world.

Objective:

This lesson plan aims to help youth workers facilitate discussions and activities to promote healthy digital engagement among young people. By the end of the session, participants should understand the importance of balance in digital usage and have practical strategies to achieve it.

Guide for Youth Workers:

- Prioritise creating a safe and non-judgmental space for discussion.
- Be mindful of your digital habits and model healthy behaviour for participants.
- Tailor the activities and discussions to the specific needs and interests of the participants.
- Encourage active participation and respect diverse perspectives.
- Provide resources and referrals for participants needing additional support with digital well-being.



LESSON PLAN

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Workshop Opening: Activity 1: Introduction</p> <ul style="list-style-type: none"> - Welcome participants and introduce the topic of balancing digital engagement. - Discuss the prevalence of digital technology in young people's lives and the potential benefits and drawbacks. - Emphasize the importance of balancing online and offline activities for overall well-being. 	10 minutes	<p>Training venue with IT equipment. Projector, overhead and PC/laptop.</p> <ul style="list-style-type: none"> - Whiteboard or flip chart - Markers - Handouts (optional) - Internet access (optional for multimedia resources) <p>Manual-Digital Sovereignty Competences for Youth Workers Unit 4.2 Balancing Digital Engagement</p>	<ul style="list-style-type: none"> - Participants will understand the significance of balancing digital engagement for overall well-being. - Participants will recognise digital technology's potential benefits and drawbacks in young people's lives. - Participants will appreciate the importance of balancing online and offline activities.
<p>Activity 2. Understanding Digital Engagement</p> <ul style="list-style-type: none"> - Facilitate a discussion on how young people engage with digital technology (e.g., social media, gaming, streaming). - Explore the positive aspects of digital engagement, such as staying connected with friends, accessing educational resources, and pursuing hobbies. - Discuss potential negative consequences of excessive digital engagement, including reduced physical activity, sleep disturbances, and social isolation. 	15 minutes	<p><u>Links online platform Digital Sovereignty Competences training course</u></p> <p><u>Unit 4. Protecting Health and Well-being</u></p> <p><u>Using Digital Technologies for Everyday Activities: QUIZ</u></p>	<ul style="list-style-type: none"> - Participants will identify how young people engage with digital technology. - Participants will articulate the positive aspects of digital engagement, including social connection and access to resources. - Participants will recognise potential negative consequences of excessive digital engagement on physical and mental health.



LESSON PLAN

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Activity 3: Identifying Signs of Imbalance</p> <ul style="list-style-type: none"> - Brainstorm with participants common signs that indicate someone may be spending too much time online (e.g., neglecting responsibilities, withdrawal from offline activities, and mood changes). - Encourage participants to reflect on their digital habits and identify any signs of imbalance they may have noticed in themselves or others. 	10 minutes	<p>Links online platform Digital Sovereignty Competences training course Unit 4.2. Balancing Digital Engagement.</p>	<p>Participants will brainstorm common signs indicating excessive digital usage and imbalance.</p> <ul style="list-style-type: none"> - Participants will reflect on their digital habits and recognise any signs of imbalance they may exhibit. - Participants will understand the importance of self-awareness in recognising and addressing digital imbalance.
<p>Activity 4: Strategies for Balancing Digital Engagement</p> <p>Present a list of practical strategies for achieving a healthy balance between online and offline activities. Including</p> <ul style="list-style-type: none"> • setting limits on screen time, designing tech-free zones or times, • engaging in physical activities or hobbies, • practising mindfulness and self-awareness, and encouraging participants to share their strategies and experiences to find balance. 	15 minutes	<p>Links online platform Digital Sovereignty Competences training course Unit 4.2. Balancing Digital Engagement.</p>	<ul style="list-style-type: none"> - Participants will acquire practical strategies to balance online and offline activities. - Participants will be able to articulate the importance of setting limits on screen time and creating tech-free zones. - Participants will share personal experiences and insights on finding Balance and fostering A collaborative learning environment.



LESSON PLAN

DESCRIPTION OF THE LEARNING ACTIVITIES	DURATION	MATERIALS	LEARNING OUTCOMES
<p>Activity 5: Interactive Activity</p> <ul style="list-style-type: none"> - Divide participants into small groups and provide them with case scenarios to depict digital engagement scenarios (e.g., a student struggling to balance schoolwork and social media and a teenager spending excessive time gaming). - Ask each group to discuss the scenario and devise a plan of action to help the individual achieve a healthier balance. - Have groups share their ideas with the rest of the class. 	15 minutes	<ul style="list-style-type: none"> - <u>Use paper and pen for individual reflections.</u> - <u>Use a whiteboard or poster paper to share answers.</u> 	<ul style="list-style-type: none"> - Participants will collaborate in small groups to analyse and discuss case scenarios depicting digital engagement challenges. - Participants will develop creative solutions and action plans to address a digital imbalance in each scenario - Participants will share their ideas with the rest of the class, promoting peer learning and exchange of perspectives.
<p>Activity 6: Conclusion and Reflection</p> <ul style="list-style-type: none"> - Summarize the key points discussed during the session. - Encourage participants to reflect on one action they can take to improve their digital balance or support others in finding balance. - Thank participants for participating and encourage them to continue the conversation outside the session. 	10 minutes		<ul style="list-style-type: none"> - Participants will summarise the key concepts and insights gained during the session. - Participants will reflect on one actionable step to improve their digital balance or support others in finding balance. - Participants will express commitment to applying the lessons learned and continuing the conversation on digital well-being outside the session.
Total duration	60-90 minutes		

5. Protecting the Environment

In an era dominated by digital technologies, the environmental impact of our digital activities has become a significant concern. This section delves into Sustainable Digital Practices, exploring the environmental implications of our digital interactions and providing insights into mitigating these impacts.

5.1 Environmental impact of digital activities

Green technology, also known as clean technology or sustainable technology, refers to any technology or process that is designed to reduce environmental impact and improve sustainability. It includes a wide range of technologies across various industries that are developed and implemented with the goal of mitigating the negative effects.

Youth workers/trainers can share with young people podcasts created by LINKS project partners: Understanding the concept of green technology podcast can be found on project's platform under Topic: Protecting Health and well being

From other side, there is also negative impact of digital technologies and youth workers/trainers have to inform young people about it. Youth workers/trainers can use the case study created by LINKS project partners that can be found on project's platform Topic 4. Case study: Understanding how digital transformation impacts the environment negatively.

Here are some additional facts which youth workers can use during own activities:

Digital technology is responsible for 4% of global greenhouse gas (GHG) emissions. Digital technology's share of global GHG emissions is rising sharply and could double by 2025 to reach 8% according to the Shift Project's report on the environmental impact of digital technology and 5G roll out.

Before landing in our pockets, our smartphones, laptops and other digital gadgets require a significant amount of materials and fossil fuels. Making a smartphone requires up to 70 different materials and 50 different metals, approximately 20 are currently recyclable. $\frac{3}{4}$ of the environmental impact of smartphones is related to their manufacture. 62% of smartphones are replaced even though they are working. Manufacturing and transporting a laptop emits between 60 and 40 kg of CO₂.

According to ADEME, digital equipment accounts for 47%% of the greenhouse gas emission. Manufacturing process has the most impact, more than its use. More information is in the article "What is the environmental impact of digital technology?" you can find [HERE](#)

We suggest to share with young people also article

[The impact digitalisation is having on the environment](#)

Youth workers/trainers can start discussion with young people from their own experience how to reduce environmental impact. This discussion can be organised in small groups and shared later with all audience or directly with the whole group of youngsters.

We suggest to discuss five ways to contribute to reducing the technology carbon footprint:

- Reduce energy consumption
- Transition to renewable energy
- Reduce e-waste
- Promote sustainable manufacturing
- Advocate for policy change

To finalise activity on the positive side, youth workers/trainers can offer to young people quiz created by LINKS project partners to better understand how digital transformation impacts the environment positively that can be found on project's platform under Topic 4.



5.2 Sustainable Digital Practices

In an era dominated by digital advancements, adopting Sustainable Digital Practices that align with environmental responsibility, personal well-being, and ethical conduct is crucial. This guide is tailored to equip you, youth workers, with the knowledge and skills necessary to navigate the digital landscape responsibly. We will guide you through this vast issue thanks to the different digital nuggets that have been created, in this section we will refer to the Possibilities and Solutions to Reduce the Environmental Impact of Digital Technologies.

In the pursuit of sustainable digital engagement, it is essential to adopt practices that not only enhance productivity but also contribute to reducing digital pollution. Here, we outline key changes and strategies that empower young individuals to navigate the digital landscape responsibly. By clicking on the link to this interactive case study you will be able to understand how to reduce digital pollution

Interactive Case Study: Understand how to reduce digital pollution
Engage in an immersive and educational experience with our Interactive Game, designed to foster awareness of how technology can pave the way for sustainable solutions in the future. Embark on a journey to explore innovative and eco-friendly technological advancements that hold the key to a sustainable future. Dive into problem-solving challenges that require participants to apply sustainable technology solutions. This hands-on approach encourages critical thinking and empowers young individuals to envision practical applications of technology for environmental conservation

Interactive Game: Understanding how technology will offer sustainable solutions for the future.

Unlock the secrets to eco-friendly digital practices with our visually appealing Infographic Resource. This resource is designed to offer actionable insights and a breakdown of practices for young individuals to reduce digital pollution in their daily lives.

Experience the power of visual learning, the combination of compelling visuals and concise information ensures that individuals can quickly grasp the key principles of reducing digital pollution and apply them effortlessly. Thanks to this digital nugget, you will discover a series of actionable steps that individuals can take to minimize their digital footprint.

Infographic Resource: Understanding how to reduce digital pollution on a small scale

Embark on a dynamic auditory experience with our Podcast, "Understanding How to Declutter Our Digital Spaces." This podcast provides insightful guidance on minimizing digital waste and offers practical tips for cultivating a sustainable and organized digital presence. The podcast strikes a balance between education and entertainment, making the learning experience enjoyable. The practical tips and strategies shared in the podcast empower listeners to take control of their digital spaces, fostering a sense of organization and environmental responsibility.

Podcast: Understanding how to declutter our digital spaces

Gain insights into why green technology is crucial for addressing environmental challenges. The video outlines the positive impact of sustainable technology practices and how they contribute to a more eco-friendly and responsible future.

Visualizations play a key role in conveying complex information with clarity. The video leverages visual elements to simplify intricate concepts, making it accessible to individuals with varying levels of familiarity with green technology. By understanding the significance of green technology, viewers are empowered to make informed and sustainable choices.

E-learning Video: Understanding the concept of green technology

6. Educational Strategies for Youth Workers

The Scenario-based learning

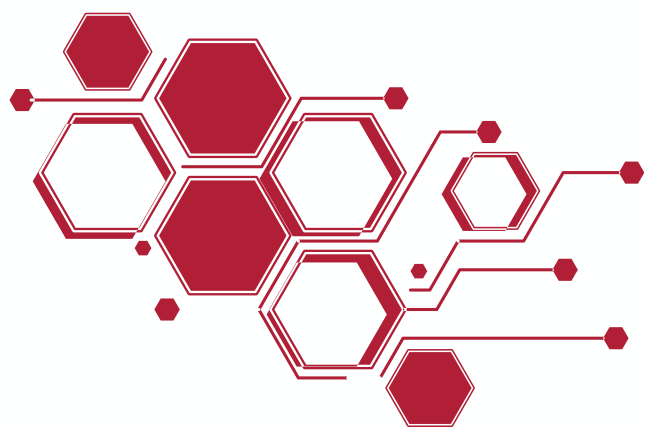
Scenario-based learning is a teaching strategy that can improve e-learning. Scenario-based learning (SBL) provides an immersive training experience where learners meet realistic work challenges and get realistic feedback as they progress since everything that happens reflects the learner's choices.

It is important to include scenarios in a learning or training module to make it more relatable for the learners.

In scenario-based learning, the learners are presented with a scenario or a situation and are then asked how to go forward from the scenario. It is a technique of teaching through storytelling. This type of teaching and learning is based on the principles of situated learning theory formulated by Lathe and Vendor in 1991. According to them, learning best takes place in the context in which it is going to be used. Scenario-based learning has a lot in common with Situated cognition. It is the similar idea that knowledge is best acquired and more fully understood when situated within its context.

Scenario-based learning is creating a safe environment where learners can have social interaction during online learning. Scenario-based learning eliminates the lack of personal one-on-one engagement with trained and qualified instructors by providing an interactive environment for active learning.

The goal of this type of learning is to identify a solution or a response to a real-world issue. Scenario-based learning can be used to give compliance training, soft skills training, professional skills training, leadership training, etc.



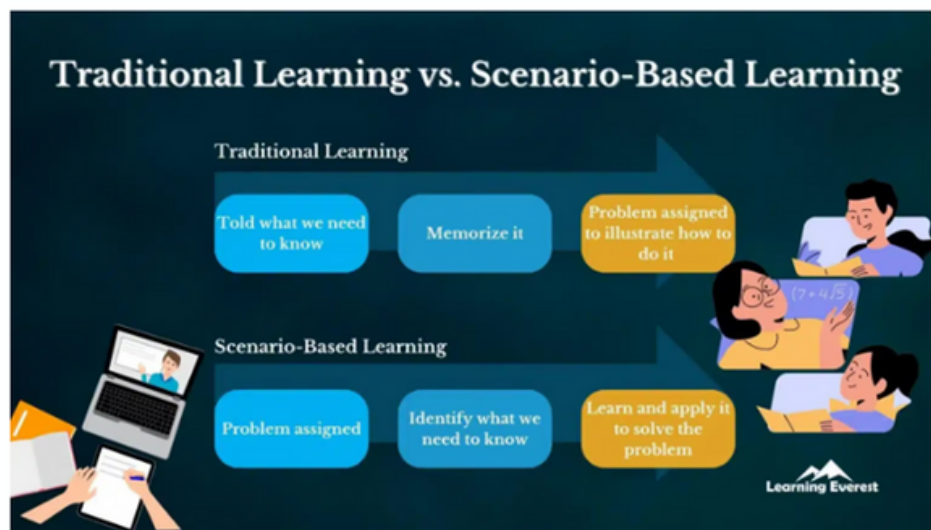
How to create scenario-based learning?

- To build a scenario, first, you need to collect information about where it takes place, who is there, and what is happening (knowing the audience helps in creating a relevant situation that helps the learners to use their knowledge in real-world situations).
- There should be an overall end conclusion to each scenario. There can be multiple correct endings to a scenario depending on learners' responses, but they too must be planned, and each path must match the learning objectives of the given course. An effective way to plan endings can be starting with the outcome and then going back to the beginning.
- Make the scenarios as real as possible, as well as the images, videos, and interactivities. One can also include resources such as articles from Wikipedia, forums, and social media groups for discussions. Also, e-learning might require to be used in good-old traditional classroom training sometimes, and therefore instructional designers should also consider a blended-learning framework to deliver scenario-based learning.
- The scenarios must force the employees or learners to employ their critical, analytical, and evaluative powers. They must encourage the employees or learners to think creatively and put themselves in the middle of the scenario before taking any action.
- Each scenario-based course should begin with a problem statement. It should generate a sense of crisis. Finding the solution to the problem should be the main motive of scenario-based learning. After the problem statement, the course branches into various ways depending upon the learner's choices. Instructional designers must provide a detailed outline of what happens in each phase while storyboarding the course.
- Scenarios should be consistent throughout the course and connect to the real-life application of that course.
- Scenarios should involve the gamification of the work like a challenge to keep learners interested throughout the course.

- Each scenario should be built previous consultation of experienced professionals like subject matter experts, managers, team leaders, and other senior members of the organization. Discuss the scenarios with them before implementing them.

Example of a real-life scenario

Instructional designers can choose real-life scenarios to make skill training easy for the employees. It can provide specific skill training. Interesting scenarios provide more fun and experiences to the learners, making the training content more engaging and memorable.



Traditional Learning Vs Scenario-based Learning Examples

How is scenario-based learning adding value to e-learning?

- Scenario-based learning incorporates storytelling into the e-learning content. It makes the e-learning content which is full of data and information, more engaging and impactful to its learners. It is highly interactive and has a high-fidelity rate due to its nature. It promotes active learning among its learners. It, therefore, enhances the process of solving problems. Here are some ways in which scenario-based learning adds value to a learning journey:
- Motivates the learners: A well-aligned scenario stimulates human curiosity. Curiosity helps humans to want to know more about what happens next. The storytelling nature of scenario-based learning intrigues human psychology. Therefore, naturally, this type of learning generates a sense of motivation in the learners.

- Prepares them for real-world situations: Learners always develop more extraordinary cognitive abilities than traditional learners. They exhibit better problem-solving skills, better memory, higher retention power, and excellent attention control. Employees who need to upskill at their jobs find scenario-based learning more appropriate as it also prepares them to solve real problems.
- Affects the thinking and behavioral patterns: Scenario-based learning enables learners to influence the behavior taken in real life and helps them achieve the desired outcomes. However, scenario-based learning must be well designed, accounting for all the variables in the learner's real life.
- Better completion rates: Scenario-based learning is exceptional for keeping the learners engaged throughout the learning journey. It cultivates more real experiences from augmented reality than virtual ones.
- Has higher recall and retention power: Visual effects are highly appreciated when it comes to learning. Therefore, by creating audio-visual techniques as a reality, scenario-based learning transforms how learners used to learn and makes it a more easily graspable form of e-learning.
- Promotes learning through experience: Scenario-based learning ensures that knowledge is fundamental and relevant to people by facilitating knowledge through expertise. It generates essential skills such as problem-solving, critical thinking, teamwork, and communication.
- Moreover, scenario-based learning is highly engaging and realistic in nature, and the learners are able to relate to the learning process because of that.

Content & image source

Hands-on activities

Hands-on activities are an effective way to engage youth in learning about data sovereignty by allowing them to actively participate in the exploration and application of concepts. Here are some elaborations on hands-on activities:

Privacy Policy Analysis: Provide youth with a variety of privacy policies from popular apps, social media platforms, or websites. In small groups or individually, have them review the policies to identify how personal data is collected, stored, and used by the service provider. Encourage them to pay attention to language, clarity, and transparency in the policies. Afterward, facilitate a discussion where they can share their findings and insights.

Data Protection Toolkit Creation: Divide youth into teams and assign each team a specific digital platform or scenario (e.g., social media, online shopping, mobile apps). Ask them to research and compile a toolkit of practical tips and strategies for protecting personal data in that context. This could include steps like adjusting privacy settings, using strong passwords, and being cautious about sharing sensitive information. Each team can then present their toolkit to the group, fostering knowledge-sharing and collaborative learning.



Privacy Impact Assessments: Introduce youth to the concept of privacy impact assessments (PIAs), which are systematic evaluations of how personal data is handled within an organization or project. Provide them with a fictional scenario (e.g., a new social media platform launching) and ask them to conduct a PIA by identifying potential privacy risks, assessing their impact, and proposing mitigation measures. This activity encourages critical thinking and problem-solving skills while highlighting the importance of proactive privacy management.

Data Breach Response Simulation: Simulate a data breach scenario where youth are tasked with responding to a fictional security incident involving personal data. Provide them with a series of prompts and challenges (e.g., notifying affected users, cooperating with authorities, improving security measures) and ask them to develop a response plan. This activity helps youth understand the consequences of data breaches and the importance of preparedness and quick action in mitigating harm.

Privacy-focused App Development: Challenge youth to design and prototype a mobile app or digital service with privacy and data sovereignty as core principles. Encourage them to consider features such as clear consent mechanisms, data minimization, encryption, and user empowerment. Throughout the design process, facilitate discussions about ethical considerations, user rights, and the trade-offs involved in balancing privacy with functionality and usability.

Data Privacy Campaign: Guide youth in planning and executing a data privacy awareness campaign targeted at their peers or the wider community. This could involve creating educational materials, organizing events or workshops, and leveraging social media to raise awareness about privacy rights and best practices. Empower youth to take leadership roles in advocating for data sovereignty and promoting a culture of privacy-consciousness in their social circles.

These hands-on activities provide practical experiences that deepen youth's understanding of data sovereignty while fostering critical thinking, collaboration, and creativity. They empower young people to become informed digital citizens who are equipped to protect their privacy and advocate for their rights in an increasingly data-driven world.



7. Resources and Tools for Youth Workers

When it comes to digital technologies, Europe is indeed largely dependent on foreign technologies and storage and processing capacities, even though it is one of the largest producers of data.

How can be achieved European digital sovereignty at the technological and industrial level?

Gaia-X aims to put together a federated infrastructure of data and solutions capable of providing technological services based on the values that unite the member countries of the Union, with the ambition of creating a true European Cloud.

This does not only mean focusing on information sharing in order to create a common and secure ecosystem for end users, providers, the public world and the entrepreneurial side, but also and above all strengthening the digital sovereignty of the EU single market.

Gaia-X's vision for the European Cloud is based on a very specific consideration: data platforms are becoming the digital twin of economic, political and social ecosystems. The ability to guarantee compliance with the fundamental principles of freedom, transparency and sovereignty in terms of data management, consequently, will determine the future of Europe and civil society.

Source : <https://magazine.wiit.cloud/gaia-x-european-cloud-perch%C3%A9-%C3%A8-importante-la-sovranit%C3%A0-dei-dati>



Source <https://www.youtube.com/watch?v=UpayPkGzgeo>

Electronic Frontier Foundation (EFF) - Security Education Companion:
Link: [Security Education Companion](#)

A resource for people who want to help their communities learn about digital security. It includes customizable educational materials.
[For the Manual]

A Guide to Digital Security Education with EFF's Security Education Companion

In the age of rapid digitalization, equipping youth workers with the tools to navigate the digital landscape is paramount. The Electronic Frontier Foundation (EFF) - Security Education Companion emerges as a robust resource tailored to the unique needs of youth workers striving to enhance their digital sovereignty competencies.

Why EFF's Security Education Companion?

Comprehensive Digital Security Education: This resource serves as a comprehensive guide, offering a plethora of customizable educational materials. It covers a spectrum of topics crucial in the digital age, from online privacy and encryption to secure communication.

Tailored for Youth Workers: Recognizing the specific challenges faced by youth workers, the Security Education Companion delves into practical aspects of digital security. It is crafted to resonate with the unique responsibilities and contexts of youth-oriented organizations.

Customizable Materials:

One size doesn't fit all. The Security Education Companion allows youth workers to adapt the materials to suit the needs of their audience. This flexibility ensures relevance and engagement in diverse educational settings.



How Youth Workers Can Utilize this Resource:

Digital Security Workshops: Conduct workshops using the pre-designed materials to educate young individuals about the importance of digital security. Tailor the content to address the specific challenges faced by the youth demographic.

Interactive Sessions: Leverage the hands-on activities provided by EFF to make digital security education interactive and engaging. Foster a culture of learning by doing, empowering youth workers to facilitate impactful sessions.

Campaigns and Outreach: Utilize the customizable resources to create targeted campaigns or outreach programs. Address prevalent digital security concerns faced by youth, such as online privacy, social media safety, and secure communication.

Direct Link to the Resource: [EFF's Security Education Companion](#)

In conclusion, EFF's Security Education Companion stands as a beacon for youth workers navigating the complexities of digital security education. Empower yourself with this comprehensive guide to foster a generation of digitally literate and secure young individuals.

Other resources and tools that could be used: (for partners if needed)

- Electronic Frontier Foundation (EFF) - Surveillance Self-Defense Guide:

Link: [Surveillance Self-Defense](#)

Description: A comprehensive guide by EFF that provides practical advice on protecting oneself from digital surveillance. It covers topics like secure communication, data protection, and privacy.



- Data Detox Kit by Tactical Tech:

Link: [Data Detox Kit](#)

Description: An interactive and user-friendly kit that guides individuals through a series of steps to enhance their digital privacy and reduce their digital footprint.

- Privacy Tools:

Link: [PrivacyTools](#)

Curated list of privacy-focused tools and services. Includes recommendations for secure messaging apps, email providers, VPNs, and more.

- Digital Security Helpline by Access Now:

Link: [Digital Security Helpline](#)

Assistance to individuals and organizations dealing with digital security issues. Youth workers can seek guidance on digital security concerns.

8.Conclusion

In conclusion, the manual "Development of the Digital Sovereignty Competences of Youth Workers" serves as a comprehensive guide for empowering youth workers with the necessary knowledge and skills to navigate the ever-evolving digital landscape responsibly. Through an exploration of various topics such as understanding the digital landscape, protecting devices, competences for safeguarding personal data and privacy, safeguarding health and well-being, and advocating for environmental protection, youth workers are equipped with practical strategies to promote digital sovereignty among the youth they serve.

Furthermore, the manual emphasizes the importance of continuous education and critical reflection in enhancing digital sovereignty competences. By fostering a deep understanding of the implications of digital technologies on privacy, health, and the environment, youth workers are better positioned to support young people in making informed decisions and advocating for their rights in the digital realm. With the resources and tools provided in this manual, youth workers can play a pivotal role in empowering the next generation to navigate the digital world confidently, responsibly, and ethically, ensuring a future where digital sovereignty is upheld and respected.