LINKS

Co-funded by the European Union

The Digital Sovereignty Competences Framework

Co-funded by
the European Union

This project has support from the European Commission by Erasmus+ program. This publication reflects the views only of the author and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Read more about

LINKS

Table of Contents

4. Introduction

5. Findings of the project survey and focus groups

6. Need of the Digital Sovereignty Competences Framework

7. Existing relevant frameworks

8. The Digital Sovereignty Competences Framework for youth workers

12. References

Introduction

The LINKS project aims to support European youth workers in achieving their own data sovereignty and enhancing their digital security skills through a new, innovative form of training content in support of digital competence building.

During the initial planning phases of this project and application, the need analysis supported the fact that there is currently no single digital sovereignty and security competence framework for Europe.

The DigComp (Digital Competence Framework) references many of the overarching and general core skills and competences related to digital security on the whole, and this output will reference this existing competence framework, but is specifically targeted towards proactive awareness of youth workers across Europe of the digital security threats which currently exist.

The Digital Sovereignty Competences Framework defines the key components of competences needed by youth workers to effectively integrate digital sovereignty and security protocols into their localized contexts, as well as to provide and validate an EU reference framework for developing and evaluating digital security competences. Digital security competences are heavily linked to generic digital competences, and not considered to be competences in their own right.

The framework targets youth workers, but is also relevant and of interest to pre-service / in-service ICT teachers and trainers and educators, as well as educational and lifelong learning policy makers, relating to the technological up-skilling and capacity building of individuals.

We expect that digital training NGOs and training organizations across Europe will adopt this framework as part of their educational assessment and teaching activities, which in the long term, will increase the awareness and encourage integration of the framework into local, regional and national digital educational bodies in European countries.

Findings of the project survey and focus groups

The Digital Sovereignty Competences Framework is based on the methodology and findings from the project survey and focus groups. It looks also to align itself with the DigComp Framework which supports long-term exploitation and sustainability as an additional, target group specific competence framework.

Project survey helped to learn about the use of technology and data protection in the digital work practices of youth workers. Youth workers need greater awareness combined with good management of digital identities, it can help limit the events caused by "inattention" of the user or the organization itself. They wrote about need of setting up and communicating remote-work security policies, about regulating personal-device use, securing communication and collaboration channels and providing vigilant IT support. They recommended to make courses available for more staff members and young people, to use more relevant examples regarding specific tasks, improve networking and sharing good and bad experiences online. It is important to keep updating and particularly with new EU documents.

Most of youth workers have not received targeted training, they make choices about online security based on own knowledge. They wrote that it is necessary to deepen these aspects for the safety of the organisations and private users and organise special trainig for Data Protection Officers.

Need of the Digital Sovereignty Competences Framework

There is growing concern that the citizens, businesses, and member states of the European Union are gradually losing control over their data, their capacity for innovation, and their ability to shape and enforce legislation in the digital environment. Against this background, support has been growing for a new policy approach designed to enhance Europe's strategic autonomy in the digital field.

Technology companies are collecting massive amounts of personal data, and concern has grown in the EU about how European citizens can recover control of their digital data in an online environment that is now primarily dominated by non-EU tech companies.

As youth work is increasingly adjusting to the digital world, we see that youth workers are also embracing new approaches. Whilst the digital is new and exciting, offering countless opportunities, it nonetheless demands improved comprehension in the context of youth work. More actions are required to map existing digital youth work practices, platforms, tools, and learning frameworks when it comes to digital sovereignty competences.

Digital sovereignty is a new concept in the digital era, commonly understood to be 'the capacity of individuals to own their private data and control its use'.

The COVID-19 pandemic has had huge effects on the daily lives of most individuals. In response, technology has been adapted to try and mitigate these effects, offering individuals digital alternatives to many of the day-to-day activities which can no longer be completed normally. Virtual socializing and online events have become commonplace and have gone a long way to keeping people from being completely isolated while in lock down.

Online education has also become the new normal in many places, as schools and universities turn to online classes to keep student education on track. Furthermore, as individuals have more flexible schedules, or more free time during the lock down, there has been a significant increase in the number of people making use of personal learning and development tools like language learning apps. Healthcare has also turned to digital solutions, and making both mental and physical healthcare available online has become more common and has been fairly successful in helping mitigate the negative effects of reduced healthcare access.

Existing relevant frameworks

Various digital pedagogical competence frameworks have been developed to support professional teachers' effective and meaningful criterion-based professional development of digital pedagogical competences.

European frameworks published in recent years outline how a digitally competent educational organisation DigCompOrg and digitally competent teaching staff DigCompEdu should look, encouraging organisations to ensure competences of their staff and to develop national solutions to ensure digital competence.

DigCompEdu is digital competence framework and has mainly as a target group university professors and staff members.
DigComp framework identifies the key components of digital competence in five areas:

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.

There is DigComp Conceptual reference model where 21 competences are pertinent to these areas. Additional dimensions outline proficiency levels, knowledge, skills and attitudes and use cases.

The Digital Sovereignty Competences Framework for youth workers

Based on survey and analysing of existing frameworks, partners of this project decided to focus on four safety topics of DigiComp and also add competences needed special for youth workers. Here are competences of DigiComp framework:

4.1 Protecting devices

To protect devices and digital content, and to understand risks and threats in digital environments. To know about safety and security measures and to have due regard to reliability and privacy.

4.2 Protecting personal data and privacy

To protect personal data and privacy in digital environments. To understand how to use and share personally identifiable information while being able to protect oneself and others from damages. To understand that digital services use a "Privacy policy" to inform how personal data is used.

4.3 Protecting health and well-being

To be able to avoid health-risks and threats to physical and psychological well-being while using digital technologies. To be able to protect oneself and others from possible dangers in digital environments (e.g. cyber bullying). To be aware of digital technologies for social well-being and social inclusion.

4.4 Protecting the environment

To be aware of the environmental impact of digital technologies and their use.
https://joint-research-centre.ec.europa.eu/digcomp/digital-competence-framework_en#ref-4-safety_

When defining basic digital competences for youth workers, it is useful to think about both the universal (DigComp competences for citizens) and specific (everyday activities in youth work) features of the resulting practical learning.

Competences for the protecting personal data and privacy

* technical digital technologies skills,
* the ability to use digital technologies in a meaningful way for working, studying and other everyday activities,
* the ability to critically evaluate digital technologies;
* to know the basic rules concerning online safety;
* to understand how online works;
* to understand what e-marketing is and how it works;
* to understand privacy and be aware of intellectual property rights;
* to know how to implement security measures;
* to develop self-efficacy using digital technologies.

Competences for the protecting devices

Protecting the computer and the smartphone with strong, up-to-date security software. If the computer or phone is infected with malicious software, other safeguards are of little help because criminals may already possess the key to all online actions. Also being sure that any operating system updates are installed is important. Youth workers should take care of all own devices. They need to be up to date, with an efficient antivirus software. Various manufacturers release updates that not only enhance the features, but also fix any security flaws that might put devices.
at risk. As a general safety rule, it is advisable to not use any other computer or device for activities that require you to 'sign in' to any of the services that you use.

Learning to spot spam and scams

Though some are easy to identify, other phishing attempts in an email, on social networking sites, or websites can look very legitimate. The only way to never fall for phishing scam is to never click on a link that has been sent. If the email says it's from a bank and has all the right logos and knows the name, it may be from the real bank or it may not be. Instead of using the link provided, finding the website and using a search engine may help preventing the scam. This way the user will know if he landed on the legitimate site and not a mocked up fake site.

Using reputable websites when making purchases

If a user doesn't know the reputation of a company that he wants to purchase from, it's important to study the site before doing so. Ask ,How are they reviewed by other users?".Do they use a secure, encrypted connection for personal and financial information?"

Staying alert

Being wary of public WiFi and thinking twice before joining an unsecured network. There are tools that can help a user have more privacy and shield during browsing activity from other users and the websites themselves on public WiFi networks.

Staying safe online

The online world has become a such rapidly changing environment that today's tips might be obsolete tomorrow. Youth workers need to be aware that the content that they consume (and it can be sometimes really lots of it) needs to be filtered. It is important to be a bit suspicious. It is relatively easy to fake things in the Internet. It is very easy to place something on the Internet that is not entirely true, or just a bunch of lies. We should take an extra care not to believe in everything we see and read in the Internet. As a good advice, we should dig deeper to distinguish what is true and what is not in case we have even slightest doubts about anything. Try to be critical about things online and thus minimise the risk involved with any online activities.

Sharing information on social network

"Information sharing describes the exchange of data between various organizations, people and technologies" (Techopedia). There are several types of information sharing:

- Information shared by individuals (such as a video shared on Facebook or YouTube);
- Information shared by organizations (such as the RSS feed of an online weather report);
- Information shared between firmware/software (such as the IP addresses of available network nodes or the availability of disk space)

All social networks (or most of them) let the users create profiles as detailed as they want. In some cases, this procedure helps the users find other users with common interests and so on. On social media like Facebook, it is possible to change the privacy settings in order to control what information is public and what information is kept only for "friends". It is important to know, however, that the social network itself has this information regardless of the privacy setting.

Usually people share age, gender, family, other interests, educational background and details related to own employment. Posting pictures or "status" is a quick way to show feelings, situations and share information. Most social networks are designed to accomplish that in the quickest way possible. Being aware of what are the things a user is sharing is really important. Sharing exposes the information that allows advertisers to track preferences and tastes of potential consumers.

GDPR

GDPR was applied to all members of the EU and EEA from May 25, 2018. It has replaced todays legislation regarding privacy in member countries currently subject to the EU Directive 95/46. GDPR is more detailed and precise in certain areas, and takes into account the challenges in the rapid evolving digital world, giving rise to privacy risks for data subjects.

References

Data protection and online privacy
https://europa.eu/youreurope/citizens/consumers/internet-telecoms/dataprotection-online-privacy/i ndex_en.htm
Techopedia https://www.techopedia.com/definition/24839/information-sharing
Step by step guidelines on setting up your computer and creating a user
https://www.wikihow.com/Use-a-Computer
Privacy rights
https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and -social