SYLLABUS ECCC

Area: **Digital competences** – DigComp 2.1
Module: DC 2.1 M4 Safety
Level: **Highly Specialised (D7)** - at highly specialised level.

Module DC 2.1 M4 Safety Level D7 includes proficiency Level 7 of the DigComp 2.1 framework in the Competence Area 4: Safety.

Competences are verified in the following competence titles:

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 a due regard to reliability and privacy.
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.
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. Protecting the environment.
   To be aware of the environmental impact of digital technologies and their use.

The competence verification is carried out in the following groups:

1. Knowledge (K).
2. Skills (S).
3. Abilities (A).

The scope verified by the ECCC exam of module DC 2.1 M4 (Level D7)

COURSE PURPOSES		LEARNING OUTCOMES		K	S	A
D7_CP1	(4.1) To acquire specialised skills of protecting devices.	DC2.1_1	Can create solutions to complex problems with limited definition that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments.			
		DC2.1_2	Can integrate my knowledge to contribute to professional practice and knowledge and guide others in protecting devices.			
D7_CP2	(4.2) To acquire specialistic knowledge about protecting	DC2.1_3	Can create solutions to complex problems with limited definition that are related to protecting personal data and privacy in digital environments, using and sharing personally identifable information protecting self and others from dangers, and privacy policies to use my personal data.			

COURSE PURPOSES		LEARNING OUTCOMES		K	S	A
	personal data and privacy.	DC2.1_4	Can integrate my knowledge to contribute to professional practice and knowledge and guide others in protecting personal data and privacy.			
D7_CP3	(4.3) To acquire specialistic knowledge of protecting health and well-being.	DC2.1_5	Can create solutions to solve complex problems with many interacting factors that are related to avoiding health -risks and threats to well-being while using digital technologies, to protect self and others from dangers in digital environments, and to the use of digital technologies for social well-being and social inclusion.			
		DC2.1_6	Can propose new ideas and processes to the field.			
		DigComp 2.1 examples.	Can create a digital campaign of possible health dangers of using a corporate account for professional reasons (e.g. bullying, addictions, physical well-being) which can be shared and used by other colleagues and professionals on their smartphones or tablets.		✓	
			Can create a blog on cyberbullying and social exclusion for digital learning platform, which helps to recognise and face up to violence in digital environments.		✓	
D7_CP4	(4.4) To acquire specialistic skills of protecting the environment.	DC2.1_7	Can create solutions to complex problems with limited definition that are related to protecting the environment from the impact of digital technologies and their use.			
		DC2.1_8	Can integrate my knowledge to contribute to professional practice and knowledge and guide others in protecting the environment.			

Practical skills, verified by the ECCC DC2.1 M4 exam, concern:

1. A computer workstation as PC / laptop equipped with a WiFi network interface and with Internet access with a minimum bandwidth of 2 Mb/s.
2. Operating system: MS Windows 7 or newer or Linux (kernel 3.0 or newer) with an account with administrator rights available to the student.
3. Programs: Acrobat Reader, CCleaner, Eraser, Wireshark, Soft Perfect Network Scanner, GIMP, OpenVPN.
4. Microsoft Office 2007 or newer (Word, Excel, Power Point).
5. Anti-virus program working in "monitor" mode with the heuristic function.
6. Libre Office suite.
7. A web browser that allows to work in private mode and allows to install add-ons such as: WOT, Adblock, Ghostery and supports plugins: Flash, Java.
8. A firewall program (the default system is also acceptable).
9. A program that encrypts directories and files (e.g. based on the EncFS library).