Cyber security

1. **Relevance:**

- Participants of the course will learn the fundamental concepts that underline the importance of cybersecurity in today's digital landscape. They learn about various types of cyber threats, such as malware, ransomware, phishing attacks, social engineering tactics, and insider threats, gaining insight into how these threats can compromise systems and data. It is important to know how we can protect the younger generation from online threats like, data phising, cybercrimes and hacking dangers. Participants can learn about tools and techniques which help students be safer and confident when using the internet.

2. **Learning outcomes:**

- Participants after the course will better understand topics like cybersecurity fundamentals, data protection and privacy and the ethical considerations in cybersecurity. They will acquire skills for the identification of cyber threats, the assessment of danger and the implementation of security policies.

3. **Planned courses and registration deadline:**

- January 2025 – February 2025 – March 2025 – July 2025 – August 2025 – September 2025 – October 2025 – November 2025
- Registration deadline: One month earlier of the course

4. **Number of participants:**

- Minimum: 7
- Maximum: 20

5. **Schedule:**

Day 1

- Introduction to Cyber Security
- Discussing goals, hopes and fears
- Welcome Session: Icebreaker activities for participants to get to know each other.
- Talking about definitions like what is data phishing, cyber crimes, hacking ect.

Day 2:

- Visiting a University specialized in cyber security, roundtable discussions with teachers about techniques and practices

- Storytelling of cyber crimes in Europe, the effect it has on education and students and how we can be more aware of it
- Practices of noticing threatening signs and dangers

Day 3

- Learning about GDPR definitions, especially related to children and younger students
- Group activity, sharing experiences and solutions
- Creating group projects about potential threats

Day 4

- Strategies for how to protect children and students for the dangers of the internet
- Learning techniques like double authentication and limited screen time
- Workshop: "Designing Internet Safety Projects" – Participants will create group projects that utilize tools and techniques for being safe on the internet.
- Peer Review: Participants will review and refine each other's project plans.

Day 5

- Assessment and Feedback
- Evaluation of learning outcomes
- Discussing strategies on gamifying the materials in order to make it easier and more interesting for younger students

Day 6

- Departure