Digital Competences for Improving Security and Defence Education (DIGICODE)

KA226 Strategic Partnerships for Higher Education: 2020-1-PL01-KA226-096192

EVALUATION REPORTS

– INTELECTUAL OUTPUT 5

Co-funded by the Erasmus+ Programme of the European Union

Warsaw, 2023

Co-funded by the Erasmus+ Programme of the European Union

AUTHORS LIST

Name, surname	Institution
GRZELAK Małgorzata	Military University of Technology, Warsaw, Poland
GONTARCZYK Mariusz	Military University of Technology, Warsaw, Poland
OWCZAREK Paulina	Military University of Technology, Warsaw, Poland
RYKAŁA Magdalena	Military University of Technology, Warsaw, Poland
RYKAŁA Łukasz	Military University of Technology, Warsaw, Poland
ZELKOWSKI Jarosław	Military University of Technology, Warsaw, Poland
MOLDOVEANU Cristian-Emil	Military Technical Academy "Ferdinand I", Bucharest, Romania
DIMITROV Dilyan	"Vasil Levski" National Military University, Artillery, Air Defence and CIS Faculty of Shumen, Bulgaria
NIKOLOV Linko	"Vasil Levski" National Military University, Artillery, Air Defence and CIS Faculty of Shumen, Bulgaria
SLAVYANOV Krasimir	"Vasil Levski" National Military University, Artillery, Air Defence and CIS Faculty of Shumen, Bulgaria
MARCHISIO Marina	University of Turin, Turin, Italy
SPINELLO Enrico	Education and Training Command and School of Applied Military Studies, Turin, Italy
ROMAN Fabio	University of Turin, Turin, Italy
SACCHET Matteo	University of Turin, Turin, Italy

Co-funded by the Erasmus+ Programme of the European Union

CONTENT

Co-funded by the Erasmus+ Programme of the European Union

1. INTRODUCTION

For many years, education systems around the world relied solely on traditional teaching methods, where relatively little adaptation of technology was sufficient to transfer knowledge (e.g., a developed multimedia presentation, etc.). However, with the beginning of 2020, the world faced the COVID-19 pandemic, a fact that radically changed the way we view both education and communication itself these days. Unsurprisingly, universities around the world were faced with a rapid transition to remote learning, where no one knew exactly how long it would take. The pandemic highlighted the critical importance of digital competence in the context of academic teaching, as in just a few weeks many institutions had to adapt to online tools, learning platforms and teaching methods that were previously little known or not widely used. Many lecturers were suddenly faced with the challenge of becoming experts in the new technology. However, the pandemic was not just a challenge, but also an opportunity to rethink the value and methods of academic teaching. It made us realize that in an era of globalization and digital revolution, the ability to adapt quickly is crucial. Improving competencies, both digital and other soft skills, has become an indispensable part of every academic's professional development. It is an investment in the future to prepare for unforeseen challenges, but also opens the door to new teaching methods and techniques that enrich the learning process and make it more engaging and effective.

The purpose of the study is to support teachers in acquiring and developing digital competencies so that they can effectively transfer knowledge and prepare students for their future path in the labor market.

The guidelines aim to:

- Provide tools and resources - provides specific tools, strategies and resources that teachers will be able to use to develop their digital skills.
- Supporting self-development - provides practical guidance for self-improvement in digital competence.
- Improving the quality of education - the use of modern tools will improve the quality of education, creating classes that are more engaging, interactive and tailored to the needs of students in the digital age.
- Increase teachers' confidence - understanding and mastering digital tools will allow them to

Co-funded by the Erasmus+ Programme of the European Union

use technology confidently and effectively in the classroom.

- Promoting a culture of lifelong learning.

The guidelines for improving digital competence are based on three pillars: knowledge, skills and attitude. The teacher in terms of:

- knowledge, acquires information and makes discernment in technological tools and trends.
- skills, are the practical dimension of digital competence, they determine how the teacher is able to use the acquired knowledge in practice.
- attitude, refers to teachers' openness, willingness and motivation to use technology, and a positive attitude toward continuous development in this field.

The guidelines are divided into two parts, the first refers to general ones that can be applied by all teachers who want to improve their digital competence, while the second refers to improving digital competence in the area of security and defense.

2. General guidelines for improving digital competence of teachers

2.1. Knowledge

1. A university teacher should learn about the latest technologies and educational tools available on the market, i.e.:

- Educational software: there are many programs and applications that have been developed with education in mind, such as Kahoot (for quizzes), edpuzzle (for video editing) and Google Classroom (for classroom management).
- Equipment: Familiarity with modern equipment such as interactive whiteboards, tablets, and specialized tools like 3D printers and VR (virtual reality) will help make lessons more interesting.
- Online resources: the use of free learning resources, such as Khan Academy, YouTube Edu, and TED-Ed, offer a rich selection of educational materials.

2. A university teacher should understand the basics of programming, if only at the block level:

- Programming is becoming increasingly popular in education, and learning the basics will allow you to better understand the digital world and use it in teaching.
- Knowledge of programming can be used to teach logical thinking, problem solving and

Co-funded by the Erasmus+ Programme of the European Union

creativity.

3. The teacher should especially pay attention to the aspect of security in the liquid and the protection of personal data:

- Online security is a key issue. It's important to know the basic rules of security, such as using strong passwords, avoiding suspicious links and keeping software up to date.
- Knowledge of data protection regulations (e.g., RODO) is essential when working with student data.

4. A university teacher should keep abreast of trends in digital education:

- The world of educational technology is dynamic. New tools, methods and approaches appear regularly.
- Keeping an eye on industry blogs, magazines and news feeds about educational technology will help keep you up to date with technology news.

5. A university teacher should participate in webinars, conferences and industry training:

- Developing knowledge in the field of educational technology is an ongoing process. In order to stay up-to-date and effectively use technology in teaching, it is worthwhile to systematically expand your knowledge, use available sources of information and exchange experiences with other teachers.

2.2. Skills

1. Teacher, should practice using a variety of educational apps and platforms:

- Use of collaboration tools: Applications i.e. Google Workspace for Education (formerly G Suite) or Microsoft Teams allow for real-time collaboration, task management or sharing of materials.
- Using LMS (Learning Management System) platforms: Moodle, Canvas or Blackboard are examples of learning management systems that allow you to create courses, tests, track student progress and much more.
- Gaining experience: Regular use of various tools will allow you to become fluent in their use and see their practical applications in education.

2. Teacher, should develop the ability to effectively use technology in teaching:

Co-funded by the Erasmus+ Programme of the European Union

- Integrating technology into the lesson plan - learning to combine learning objectives with appropriate digital tools is a valuable part of supporting the learning process, where technology helps impart knowledge rather than hinders it.
- Tailor technology to students' needs - the use of technology should be tailored to students' diverse learning styles and needs so that it supports their acquisition of knowledge, skills and competencies.
- Evaluating tools: regularly evaluating the effectiveness of the tools used and adapting them to the needs of the students and the specifics of the subject, is key to effective education.

3. The teacher should learn to design lessons using new digital tools:

- Instructional Design: Think about what digital tools can help achieve specific learning goals.
- Interactivity: Use technology to create interactive lessons that engage students and promote active participation.
- Real-time Feedback: Use tools that provide immediate feedback to students, which can increase their engagement and motivation.

4. The teacher should establish and maintain contacts with other teachers in the network to exchange experiences:

- Networking within online communities: Use groups, forums or communities dedicated to teachers on platforms such as Facebook, LinkedIn or specialized educational websites.
- Collaborate with other teachers - will allow sharing of proven practices, classroom ideas and solutions to technology-related problems in education.

2.3. Responsibility and autonomy

1. The teacher should be open to innovation:

- Willingness to experiment: Don't be afraid to test new tools or methods. Every failure is a learning opportunity, and success can open the door to new educational opportunities.
- Understanding the benefits: Technology is not an end in itself, but a tool for better learning. Understanding this is the key to acceptance and willingness to implement innovations.

2. The teacher should constantly develop himself:

- Self-study: Take advantage of online courses, webinars, tutorials and resources to help you

Co-funded by the Erasmus+ Programme of the European Union

expand your digital competencies.

- Understand that learning is a process: technology changes, and new tools and methods appear regularly. It is crucial to continuously improve and update your knowledge.

3. The teacher should have critical thinking towards technology:

- Evaluating tools: Not every tool or application is appropriate for every classroom or situation. It is important to skillfully evaluate and select those that will actually provide educational benefits.
- Ethical use of technology: Understand and follow the principles of security, privacy, and responsible use of technology.

4. The teacher should cooperate and share knowledge:

- Building community: Collaborating with other teachers, sharing experiences and best practices is essential for effective technology implementation in education.
- Support for others: If you have gained skills or knowledge in a certain area, share it with your colleagues, creating a culture of community and support.

5. The teacher should have a positive attitude towards challenges:

- Resilience (mental toughness): Not every technology experiment will be successful. It is important not to be discouraged by failures, but to treat them as valuable lessons.
- Proactive problem solving: When you encounter difficulties, look for solutions, ask questions, use forums or support groups.

3. Guidelines for improving digital competence for teachers in the security and defense education

The digital world is constantly changing and threats are evolving. Teachers must not only stay up-to-date, but also pass on this knowledge to their students so that together they can create a safer online learning environment. Proper management of digital security skills is not just about theoretical knowledge, but also about practical application of this knowledge in everyday life. Regular practice and improvement of these skills is the key to protecting yourself and others in a rapidly changing digital environment. Attitude towards digital security is not just a matter of knowledge or skills, but also the values and beliefs that guide our actions. For teachers, who act as guides for younger generations in the digital world, the right attitude is key to creating a safe

Co-funded by the Erasmus+ Programme of the European Union

and supportive educational environment.

3.1. Knowledge

Digital security is not just about malware. There are many ways cybercriminals can attack, and educators need to be aware of the variety of these threats to better protect themselves and their students.

1. The teacher should understand the basic digital risks, i.e:

- Viruses - computer programs that can replicate themselves by transferring from one device to another, often through e-mail attachments or infected websites. They can cause system damage or data theft.
- Malware - includes various types of malware, such as spyware (spyware), ransomware (ransomware) and Trojans. They often infiltrate systems to steal information or cause other damage.
- Phishing - attacks involving the impersonation of a credible source (e.g., a bank, a social networking site) to defraud login credentials, credit information, etc.
- DDoS attacks - which involve overloading a server with multiple requests, which can lead to it crashing or shutting down. For teachers, this is important, especially if they use online platforms for teaching.
- Man-in-the-Middle (MitM) attacks - Cyber criminals intercept and modify communications between two parties without their knowledge. For example, if a teacher logs into an educational platform, an attacker can intercept his or her login credentials.

2. The teacher should be familiar with security tools for digital security i. e.:

- Antivirus software - allows you to scan your computer for known viruses and malware, offering to remove them. Regular updates are the key to effectiveness.
- Firewalls - They act as a shield, blocking unauthorized access to a computer or network.
- VPNs (Virtual Private Networks): Allow you to surf the Internet anonymously and securely by encrypting your connection.
- Password Managers: Tools that help store and generate strong, unique passwords for various services.

3. The teacher should understand the principles of cyber hygiene:

Co-funded by the Erasmus+ Programme of the European Union

- Regular updates - Software, operating systems and applications should be kept up-to-date to protect against new threats.
- Caution with e-mail - Avoid opening attachments or clicking on links from unknown senders.
- Two-step authentication - Enabling this feature where possible further secures accounts from unauthorized access.

4. The teacher should be knowledgeable about cybercrime:

- Understanding motives: Some attack for profit, some for fun, and some for political or ideological reasons.
- Recognizing social engineering techniques: Cybercriminals often use psychological manipulation, such as social engineering, to trick people into providing information or inducing them to perform certain actions.

3.2. Skills

1. The teacher should use the Internet safely:

- Should use an encrypted connection - should always use sites that use HTTPS, which indicates a secured connection. Search engines often mark them with a padlock icon.
- He should be careful with links - he should never click on suspicious links, especially those received by e-mail from unknown senders. Before clicking, he should check by hovering the cursor over the link to see where it actually leads.
- Should use search engines from reputable companies - Reputable search engines such as Google and Bing have built-in mechanisms to warn of potentially harmful sites.

2. The teacher should use protection tools:

- Can configure antivirus software - should have knowledge of how to set up real-time scanning, how to regularly update virus databases and how to perform full system scans.
- Should be familiar with firewall settings - Know basic firewall functions, such as blocking and allowing outgoing and incoming connections, and creating rules for specific applications.
- Portafi to configure a VPN - Knowledge of how to choose a VPN provider, connect to a

Co-funded by the Erasmus+ Programme of the European Union

server, and disconnect when a session ends.

3. The teacher should educate others: students, colleagues, etc.:

- He should create educational materials - developing presentations, instructional videos or quizzes on digital security.
- Should conduct workshops - Organizing interactive sessions for students to learn how to recognize and deal with threats.

4. Teacher should have the ability to manage data and privacy online:

- Should securely store data - Should use encrypted hard drives and cloud services, and back up important data regularly.
- Should use access restriction - Set passwords for key documents and use access control features to ensure that only the right people can access them.
- Should understand privacy laws: Knowledge of data protection laws and know what rights students have regarding data collected at the university.

3.3. Responsibility and autonomy

1. The teacher should be responsible and aware:

- They should take responsibility for their own actions - they should understand that every step in the online environment - from opening an email to clicking on a link - has consequences. Teachers should adopt an attitude of caution and reflection before acting online.
- Should educate by example - Should strive to be a role model for students through appropriate online behavior, such as using strong passwords, avoiding suspicious links and sharing best practices.

2. A teacher should have respect for the privacy of others:

- Should apply student data protection - Always ensuring that student information is stored securely and only appropriate people have access to it.
- He should respect digital boundaries - he should refrain from uninvited actions, such as tagging students in photos on social media without their permission or invading their online privacy.

3. The teacher should be ready for continuous learning:

Co-funded by the Erasmus+ Programme of the European Union

- Adaptability - should be ready to adapt to new tools, technologies and teaching methods in the digital environment.
- He or she should initiate the search for knowledge in search of knowledge: Regularly follow current digital security news, attend training courses and use available resources to stay up-to-date.

4. Teacher should cooperate and communicate with other teachers:

- He should cooperate with other teachers - sharing knowledge and experiences, creating joint strategies and plans for school safety.

5. Teacher should be proactive in approaching threats:

- Should monitor and respond: Regularly check systems and learning tools for potential threats and respond quickly to any incidents.
- Should shape a culture of safety - Support and promote safe behavior practices among students and teachers so that they become an everyday occurrence.

Co-funded by the Erasmus+ Programme of the European Union