

# The Pedagogical Essence And Content Of The Problem Of Developing Students' Educational Competencies In Digital Culture And Information Security

**Boltayeva Guzal Komilovna**

Senior Lecturer

Urgench RANCH University of Technology

E-mail: [boltayevagozal334@gmail.com](mailto:boltayevagozal334@gmail.com)

ORCID: 0009-0001-4767-2897

**Abstract:** The article examines the pedagogical essence and content of developing students' educational competencies in digital culture and information security within the context of the digital transformation of education. It analyzes the theoretical foundations of digital culture, media and information literacy, cybersecurity awareness, and responsible digital citizenship. Particular attention is paid to competence-based, learner-centered, and activity-oriented approaches that facilitate the formation of students' digital knowledge, skills, values, and ethical behavior. The study also highlights the role of educational institutions in fostering a safe digital learning environment through innovative pedagogical methods and digital technologies. The findings emphasize that the development of digital culture and information security competencies contributes to students' critical thinking, responsible online behavior, and lifelong learning in the information society.

**Keywords:** digital culture, information security, educational competencies, digital citizenship, media and information literacy, cybersecurity, digital ethics, competence-based approach, digital learning environment, critical thinking.

## Introduction

The rapid development of digital technologies has fundamentally transformed educational systems worldwide, creating new opportunities as well as new challenges for teaching and learning. The widespread use of the Internet, cloud computing, artificial intelligence, mobile technologies, and social media has significantly expanded students' access to educational resources and digital communication. However, these technological advances have also increased exposure to cyber threats, misinformation, cyberbullying, identity theft, data privacy violations, and other digital risks. Consequently, preparing students to use digital technologies safely, responsibly, and effectively has become one of the strategic priorities of modern education.

Digital culture extends beyond the ability to operate technological devices; it encompasses a system of knowledge, values, ethical norms, communication practices, and responsible behavior in the digital environment. Likewise, information security education is no longer limited to technical protection mechanisms but includes the formation of digital responsibility, media literacy, critical evaluation of information, and awareness of cybersecurity risks. International organizations such as UNESCO, UNICEF, the OECD, and the European Commission emphasize that digital competence and information security should be regarded as key twenty-first-century competencies essential for sustainable education and lifelong learning. From a pedagogical perspective, the development of educational competencies in digital culture and information security requires a systematic and interdisciplinary approach. Competence-based education integrates cognitive, practical, social, and ethical dimensions, enabling students not only to acquire digital knowledge but also to apply it responsibly in authentic contexts. Therefore, educational institutions should create learning environments that encourage critical thinking, collaborative learning, digital creativity, and ethical decision-making while ensuring students' online safety.

The pedagogical essence of this problem lies in designing effective educational strategies that integrate digital literacy, cybersecurity awareness, media and information literacy, and digital ethics into both curricular and extracurricular activities. Such an approach contributes to the formation of responsible digital citizens capable

of making informed decisions, protecting personal and public information, and participating actively in the digital society.

### **Methodology**

The development of students' educational competencies in digital culture and information security has emerged as a major interdisciplinary problem in contemporary pedagogy. The expansion of digital learning platforms, social networks, artificial intelligence systems, mobile applications, and cloud-based services has changed the ways in which students obtain information, communicate, construct knowledge, and participate in social life. Consequently, digital competence can no longer be interpreted merely as the technical ability to operate devices or software. It should be understood as an integrated system of knowledge, practical skills, attitudes, values, ethical norms, and behavioral strategies that enables students to participate in digital environments safely, critically, creatively, and responsibly.

Theoretical perspectives on this issue demonstrate that the concepts of digital literacy, digital culture, media and information literacy, information security, and digital citizenship are closely interconnected. Although these concepts emerged within different academic traditions, their pedagogical content converges around several common components: critical information evaluation, safe technological behavior, ethical communication, personal data protection, content creation, social responsibility, and active participation in digital society.

One of the earliest influential interpretations of digital literacy was proposed by Paul Gilster, who described it primarily as the ability to understand and use information presented through computers and digital technologies [1]. Gilster's interpretation shifted scholarly attention from the mechanical use of computers toward the meaningful comprehension and evaluation of digital information. His approach established an important theoretical principle: a digitally literate person should not merely access information but should also interpret its meaning, assess its reliability, and use it purposefully.

Douglas Belshaw subsequently expanded this interpretation by presenting digital literacy as a plural and context-dependent phenomenon. He identified eight interrelated elements of digital literacies: cultural, cognitive, constructive, communicative, confident, creative, critical, and civic dimensions [2]. Belshaw's model is pedagogically significant because it rejects the idea that digital competence consists of a fixed collection of technical operations. Instead, the model emphasizes that students' digital practices depend on cultural context, communication goals, social relationships, and personal responsibility.

From Belshaw's perspective, the cultural element involves understanding the norms of specific digital environments; the cognitive element concerns comprehension and conceptual knowledge; the constructive element refers to creating new meaning from digital resources; and the communicative element involves effective participation in networked interaction. The critical and civic dimensions are particularly relevant to information security education because they enable students to recognize manipulation, evaluate digital content, respect the rights of other users, and participate responsibly in online communities.

This position suggests that the pedagogical essence of digital culture lies in integrating technological knowledge with critical thinking and value-based education. Therefore, digital culture should be developed through interdisciplinary learning activities rather than confined exclusively to informatics or information technology classes.

UNESCO's Media and Information Literacy framework represents one of the most comprehensive international approaches to the development of students' competencies in the digital information environment. UNESCO combines media literacy and information literacy within a unified conceptual structure and emphasizes individuals' ability to access, analyze, critically evaluate, use, create, and disseminate information through different media channels [3].

According to this approach, learners must understand how information and media institutions operate, how messages are constructed, whose interests they represent, and what ethical consequences arise from producing or sharing content. Media and information literacy therefore includes both cognitive and axiological components. Students should be able to recognize disinformation, propaganda, hate speech, stereotypes, commercial manipulation, and algorithmically amplified content. At the same time, they should understand freedom of expression, privacy, intellectual property, cultural diversity, and responsibility for the consequences of online communication.

UNESCO's position is especially important for defining the pedagogical content of information security. In this framework, security is not reduced to antivirus software, passwords, or technical protection. It also involves protection against cognitive manipulation, harmful content, discriminatory discourse, and unethical information practices. Consequently, students' information security competence should include the ability to verify sources, distinguish fact from opinion, detect emotional manipulation, identify fabricated evidence, and avoid spreading unverified information.

The UNESCO framework also emphasizes the role of educators. A teacher is expected not only to use digital tools but also to organize learning situations in which students investigate media messages, compare information sources, produce ethical digital content, and reflect on their own media behavior. This position supports the integration of project-based learning, discussion, fact-checking exercises, digital storytelling, and media analysis into educational practice.

The European Digital Competence Framework for Citizens, known as DigComp, systematizes digital competence into five major areas: information and data literacy; communication and collaboration; digital content creation; safety; and problem-solving [4]. This classification provides an important methodological basis for designing the content, criteria, and indicators of students' digital competencies.

The first area, information and data literacy, covers searching, filtering, evaluating, and managing digital information. Its pedagogical significance lies in developing students' ability to formulate information needs, select suitable search strategies, assess the credibility of sources, and organize collected data.

The second area, communication and collaboration, includes interaction through digital technologies, online participation, digital identity management, and netiquette. These competencies form the social and communicative dimension of digital culture. They help students understand that online communication is governed by moral and legal norms similar to face-to-face interaction.

The third area, digital content creation, encompasses the production and modification of digital materials, copyright awareness, licensing, and basic programming principles. From a pedagogical perspective, content creation transforms learners from passive consumers into active and responsible producers of information.

The fourth area, safety, directly addresses device protection, personal data and privacy, health and well-being, and environmental awareness. This area demonstrates that information security competence is multidimensional. It includes technical protection, protection of identity and privacy, prevention of psychological harm, maintenance of healthy digital habits, and awareness of the ecological impact of technologies.

The fifth area, problem-solving, involves identifying technological needs, selecting appropriate digital solutions, creatively using technologies, and recognizing personal competence gaps. This component supports learner autonomy and continuous self-development.

The updated DigComp framework also addresses emerging challenges such as artificial intelligence systems, datafication, algorithmic decision-making, misleading information, and digital well-being. Therefore, the framework may serve as a diagnostic and curriculum-design instrument for determining the expected outcomes of digital culture and information security education.

## **Results and Discussion**

UNICEF scholars approach digital literacy from a child-centered and rights-based perspective. Their studies emphasize that children's digital experiences are shaped by age, social environment, access conditions, family support, educational opportunities, and vulnerability to online risks [5]. UNICEF defines children's digital literacy as a set of knowledge, skills, attitudes, and values that enables children to engage with digital environments in ways that are safe, meaningful, empowering, and appropriate to their development.

An important contribution of UNICEF's approach is the rejection of a purely restrictive model of online safety. Complete avoidance of the internet cannot provide sustainable protection because children require digital participation for education, communication, creativity, and future professional development. The pedagogical objective should therefore be to balance protection, participation, and empowerment.

This approach implies that students should gradually learn to recognize risks, seek help, report abuse, manage privacy settings, respond to cyberbullying, and make informed decisions. Teachers and parents should not merely prohibit online practices but should explain their consequences, model responsible behavior, and create conditions for open communication about digital problems.

UNICEF also emphasizes that child online protection is a shared institutional responsibility. Schools need clear policies for reporting cyberbullying, online harassment, privacy violations, and exposure to harmful content. Students should know whom to contact and should feel confident that their concerns will be addressed without blame or humiliation. Thus, psychological safety and trust become important conditions for information security education.

Michael Ribble's theory of digital citizenship has significantly influenced pedagogical discussions of responsible technological behavior. Ribble defines digital citizenship as the norms of appropriate and responsible technology use and identifies nine major elements: digital access, commerce, communication and collaboration, etiquette, fluency, health and welfare, law, rights and responsibilities, and security and privacy [6].

The educational importance of this framework lies in its integration of technical, social, legal, ethical, and health-related issues. For example, digital etiquette concerns respectful communication; digital law addresses copyright, cybercrime, plagiarism, and unlawful access; digital rights and responsibilities explain freedom of expression, privacy, and accountability; and digital security and privacy include personal data protection and preventive cybersecurity practices.

Ribble's approach indicates that information security competence cannot be formed through occasional warnings alone. It requires a planned educational process involving explanation, modeling, guided practice, reflection, and evaluation. Students should encounter realistic scenarios such as suspicious messages, fake accounts, unauthorized sharing of photographs, plagiarism, online insults, and password theft. Through case analysis and role-playing, they can learn to assess the ethical and security consequences of possible actions. Sonia Livingstone's research highlights the relationship between children's digital opportunities, skills, and risks. She argues that increased internet use can expand educational and participatory opportunities, but it may also increase exposure to certain risks [7]. The solution is not simply to reduce digital participation; rather, children's skills, resilience, and support systems should be strengthened.

Livingstone's position is important because it distinguishes between risk and harm. Exposure to a risky situation does not always result in actual harm, since outcomes depend on the child's age, psychological resilience, digital competence, social support, and the response of adults. This distinction allows educational institutions to develop differentiated preventive measures instead of applying uniform restrictions to all students.

Her research also shows that students require opportunities to discuss their online experiences. When digital safety education is based only on fear, prohibition, or punishment, students may hide problems from adults. In contrast, dialogical pedagogy encourages learners to report cyberbullying, uncomfortable communication, manipulation, and privacy violations. Therefore, trust-based teacher-student communication should be regarded as a methodological condition for information security education.

The OECD Learning Compass 2030 presents education as a process of developing the knowledge, skills, attitudes, and values necessary for individual and collective well-being [8]. A central concept in this model is student agency, understood as learners' capacity to set goals, make responsible decisions, reflect on their actions, and influence their environment.

Applied to digital culture, student agency means that learners should not remain passive recipients of ready-made digital content or automated recommendations. They should understand how digital systems influence attention, choices, opinions, and behavior. They should also be able to regulate their digital habits, select appropriate tools, evaluate consequences, and contribute to a safer digital community.

The OECD's concept of transformative competencies—creating new value, reconciling tensions and dilemmas, and taking responsibility—also enriches the pedagogical interpretation of digital culture. Creating new value involves producing useful and ethical digital content. Reconciling tensions requires balancing openness with privacy, freedom of expression with respect for others, and technological convenience with human autonomy. Taking responsibility includes anticipating the consequences of digital actions and accepting accountability for them.

The reviewed scholarship demonstrates that information security competence should be considered an integrative pedagogical construct consisting of several interrelated components.

The cognitive component includes knowledge of cyber threats, privacy principles, digital rights, copyright, data protection, and safe online communication. The operational component includes practical abilities such

as creating secure passwords, enabling multifactor authentication, identifying phishing attempts, managing privacy settings, checking links, updating software, and reporting abuse.

The critical-analytical component involves evaluating sources, detecting misinformation, understanding persuasive techniques, recognizing manipulated images and videos, and questioning algorithmic recommendations. The axiological component includes respect for dignity, privacy, intellectual property, cultural diversity, and the rights of other users. The behavioral component is reflected in responsible communication, cautious sharing, ethical content production, and adherence to security rules. Finally, the reflexive component enables students to assess their own digital habits, identify mistakes, and consciously improve their behavior.

These components indicate that the development of information security competence requires the integration of instruction and education. Knowledge about cybersecurity becomes pedagogically meaningful only when it is transformed into stable attitudes and everyday behavioral practices.

The reviewed theories support the use of active, contextualized, and learner-centered pedagogical methods. Project-based learning can be implemented through activities such as creating safe-internet guides, anti-cyberbullying campaigns, fact-checking projects, and digital citizenship codes. Case-study methods enable students to examine realistic incidents involving phishing, identity theft, plagiarism, online harassment, or harmful content.

Simulation-based learning may be used to practise responding to suspicious messages, privacy breaches, or compromised accounts. Collaborative learning supports discussion of ethical dilemmas, while reflective journals and electronic portfolios help students evaluate their own digital development. Gamification can increase motivation, although it should not oversimplify serious security and ethical problems.

Assessment should also be multidimensional. Traditional tests can measure theoretical knowledge but cannot fully reveal responsible digital behavior. Therefore, diagnostic tools should combine tests, observation, scenario-based assignments, project assessment, self-assessment, peer assessment, and portfolio analysis. Criteria may include the accuracy of risk identification, appropriateness of proposed protective actions, ethical reasoning, source evaluation, collaboration, and reflective awareness.

The literature demonstrates broad agreement that digital competence is not a narrowly technological construct. Gilster emphasizes critical comprehension of digital information; Belshaw highlights its cultural, communicative, creative, and civic dimensions; UNESCO integrates media analysis, information ethics, and democratic participation; DigComp systematizes knowledge, skills, and attitudes across information, communication, creation, safety, and problem-solving; UNICEF focuses on child rights, empowerment, protection, and developmental appropriateness; Ribble develops the concept of responsible digital citizenship; Livingstone reveals the relationship among opportunities, risks, skills, and resilience; and OECD emphasizes agency, responsibility, and transformative competence.

Despite differences in terminology, these perspectives converge on the idea that students should become conscious, critical, ethical, safe, creative, and socially responsible participants in digital society. Accordingly, the pedagogical essence of developing competencies in digital culture and information security lies in transforming fragmented technological knowledge into an integrated personal quality reflected in students' thinking, values, decisions, communication, and everyday digital behavior.



The literature also indicates that effective competence development requires a whole-school approach involving curriculum integration, teacher professional development, safe institutional policies, cooperation with families, psychological support, practical learning, and continuous assessment. Therefore, the problem should not be assigned exclusively to computer science teachers. It constitutes a shared educational responsibility of teachers, school leaders, psychologists, parents, communities, technology providers, and policymakers.

### Conclusion

The development of students' educational competencies in digital culture and information security represents one of the most significant priorities of contemporary educational reform. The study demonstrates that these competencies are multidimensional, encompassing digital literacy, information security awareness, media

literacy, critical thinking, digital ethics, and responsible online behavior. Their successful formation depends on the integration of innovative pedagogical methods, digital educational technologies, competence-based instruction, and continuous educational support.

Educational institutions play a crucial role in creating a secure and inclusive digital learning environment that enables students to acquire not only technological skills but also ethical values and responsible digital behavior. Active learning strategies, project-based learning, case studies, collaborative activities, and digital simulations significantly enhance students' ability to recognize digital threats, evaluate information critically, and make informed decisions in virtual environments.

In conclusion, the systematic development of educational competencies related to digital culture and information security prepares students for active participation in the digital economy and knowledge society. Future educational research should focus on integrating artificial intelligence, adaptive learning technologies, and international digital competence frameworks into national educational systems to further strengthen students' digital resilience, cybersecurity awareness, and lifelong learning competencies.

## References

1. Gilster, P. *Digital Literacy*. New York: Wiley Computer Publishing, 1997.
2. Belshaw, D. A. J. *The Essential Elements of Digital Literacies*. Durham: Durham University, 2012.
3. UNESCO. *Media and Information Literate Citizens: Think Critically, Click Wisely! Media and Information Literacy Curriculum for Educators and Learners*. Paris: UNESCO, 2021.
4. Vuorikari, R., Kluzer, S., and Punie, Y. *DigComp 2.2: The Digital Competence Framework for Citizens—With New Examples of Knowledge, Skills and Attitudes*. Luxembourg: Publications Office of the European Union, 2022.
5. Nascimbeni, F., and Vosloo, S. *Digital Literacy for Children: Exploring Definitions and Frameworks*. Florence: UNICEF Office of Research—Innocenti, 2019.
6. Ribble, M. *Digital Citizenship in Schools: Nine Elements All Students Should Know*. 3rd ed. Eugene, OR: International Society for Technology in Education, 2015.
7. Livingstone, S., and Haddon, L. *Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective*. Bristol: Policy Press, 2012.
8. OECD. *OECD Learning Compass 2030: A Series of Concept Notes*. Paris: Organisation for Economic Co-operation and Development, 2019.
9. UNICEF. *Child Online Protection in and through Digital Learning*. Geneva: UNICEF Regional Office for Europe and Central Asia, 2022.
10. Ferrari, A. *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe*. Luxembourg: Publications Office of the European Union, 2013.