Archipel Jounrla
E-ISSN : 3124-6621
Vol.1.No.2 October 2025
https://ojsap.com/index.php/archipel/index
DOI : https://doi.org/10.65739/archipel.v1i2.15

# Digital Literacy and Cybersecurity for Teachers and Students in the Era of Hybrid and Virtual Education

**Eni Setyo Rahayu**
[1] Univ Diponegoro Semarang, Indonesia

Email: enisetyorahayu@gmail.com

Submit : September 10, 2025
Revised : October 10, 2025
Accepted: October 20, 2025
Published : October 25, 2025

**ABSTRACT**

*The transformation of education in the digital era has demanded the integration of digital literacy and cybersecurity as two fundamental aspects for the sustainability of hybrid and virtual learning systems. This study uses a qualitative approach with a literature review method that examines various academic sources, educational policies, and legal frameworks related to digital competency and data protection. The results of the study indicate that digital literacy functions as a basic capability encompassing technological, cognitive, and ethical dimensions, while cybersecurity plays a role as an instrument of legal protection for digital activities in the educational space. Teachers and students have a legal and moral responsibility to maintain information security, avoid privacy violations, and uphold the principles of academic integrity in the cyber environment. The discussion emphasizes the need for systematic integration of digital literacy and cybersecurity in national education policy to create a safe, inclusive, and sustainable learning ecosystem. Strengthening the digital legal capacity of educators and students is a strategic step in building a learning culture based on ethics, responsibility, and protection of digital rights. In conclusion, digital literacy and cybersecurity are not merely technological necessities, but normative foundations that guarantee the sustainability and legality of education in the global digital era.*

***Keywords:*** *Digital literacy, Cybersecurity, Hybrid education*

## INTRODUCTION

The transformation of education in the digital era marks a major shift in the paradigm of learning and teaching, where technology is no longer merely a tool but has become the primary medium mediating the entire educational process. The development of hybrid learning and virtual learning systems creates new spaces for academic interactions that transcend geographical and temporal boundaries, but also demands complex digital competencies from both teachers and students. Teachers are required to manage virtual classrooms with pedagogical skills that are adaptive to technology, while students are expected to navigate various digital platforms independently and productively. This phenomenon indicates that digital literacy has shifted from mere technical skills to epistemological competencies that involve a critical understanding of information and digital ethics. Prensky (2010) emphasized that the digital native generation requires pedagogical support relevant to the digital ecosystem so that their higher-order thinking skills can develop optimally. Therefore, teachers play a crucial role as digital literacy facilitators who not only teach the use of technology but also foster a reflective attitude towards its implications for the learning process. Technology-oriented education needs to ensure that mastery of digital tools is balanced with an awareness of the meaning, responsibilities, and risks of their use. This shift indicates that digital literacy is no longer optional, but rather a prerequisite for educational success in the 21st century.

*This is an open access article distributed under the terms of the*
*Creative Commons Attribution 4.0 International License* ***(CC BY 4.0)****.*
*Copyright © 2025 The Author(s). Published by Archipel: Journal of Indonesian Interdisciplinary Studies.*

Cybersecurity awareness is a crucial dimension of digital literacy that is often overlooked, especially among teachers and students who use online platforms without understanding the associated risks. A UNESCO study (2022) showed that low knowledge of digital security leaves many educators vulnerable to threats such as phishing, malware, and data privacy breaches. Teachers who lack a grasp of basic cybersecurity principles can inadvertently transmit unsafe digital practices to their students, creating a chain of vulnerabilities within the education ecosystem. Meanwhile, students, as active internet users, often become easy targets for digital exploitation due to their curiosity and lack of awareness of hidden threats in cyberspace. This situation illustrates that increasing cybersecurity awareness is not merely a technical issue but also an ethical and pedagogical one that impacts the quality of education. As stated by Livingstone and Helsper (2010), the ability to protect oneself in the digital space is an essential part of media literacy in shaping critical and responsible digital citizens. Unpreparedness to face cyber risks has the potential to undermine trust in online learning systems and weaken learning motivation. Therefore, building a culture of digital security needs to be an integral part of technology-based education policies.

Integrating cybersecurity into the educational curriculum requires a systemic approach involving policy planning, professional training, and pedagogical design relevant to the digital needs of this century. The Digital Competence for Educators (DigCompEdu) framework developed by the European Commission (2017) emphasizes the importance of digital security competencies for teachers as part of educational professionalism. However, many educational institutions still treat digital literacy fragmentarily, limited to the ability to use devices or applications without emphasizing aspects of data protection and digital ethics. This imbalance results in the implementation of digital learning that is not fully secure or sustainable due to a weak cybersecurity foundation at both teacher and student levels. Curricula that do not prioritize digital security create systemic risks that can compromise academic integrity and the credibility of educational institutions. Furthermore, the integration of cybersecurity needs to be adapted to the socio-cultural context of schools to enable the internalization of the values of digital responsibility from an early age. The involvement of teachers as models of ethical and safe digital behavior is a key factor in building collective awareness in the educational environment. Thus, strengthening a comprehensive digital curriculum will strengthen the foundation of education towards an adaptive, secure, and globally competitive system.

Improving teacher capacity is a strategic element in bridging the gap between digital literacy and cybersecurity in educational institutions. Teachers hold dual roles as users and developers of a healthy digital ecosystem, making their competence in managing data, identifying cyber threats, and training students crucial. Research by Redecker (2019) shows that teachers with high levels of digital competence are better able to minimize security risks in online learning and increase the effectiveness of virtual collaboration. Cybersecurity-based digital literacy training needs to be designed not only as a technical activity, but also as a process of building professional awareness regarding digital ethics and privacy protection. A weakness in teacher training often lies in an excessive focus on software usage without an understanding of broader security implications. Therefore, educational institutions need to provide professional development programs that emphasize a balance between technological skills, ethical reflection, and cyber risk preparedness. When teachers have a sufficient understanding of digital security, they can consistently transmit safe behavior patterns to students in all online learning activities. Such a strategy will create a digital education ecosystem that is resilient to cyber threats and adaptive to technological change.

While teachers play a structural role in building a digital security culture, students are the primary actors who interact most frequently with cyberspace in both learning and entertainment contexts. Technology usage patterns that are not accompanied by digital security literacy can expose students to risky content, misinformation, or digital social attacks such as cyberbullying. Research by Livingstone et al. (2017) highlights the importance of participatory digital security education, where students are actively involved in understanding and solving cybersecurity issues in their environment. This approach allows students to develop a sense of ownership over their own digital security and fosters collective responsibility for safeguarding the school's cyberspace. Furthermore, critical thinking skills regarding information sources and awareness of digital footprints are essential components of 21st-century literacy competencies. Teachers need to facilitate this process through learning that emphasizes collaboration, reflection, and hands-on practice using secure digital platforms. Thus, strengthening students' cybersecurity capacities not only improves digital safety but also shapes ethical and responsible digital characters.

The development of hybrid and virtual learning systems requires the consistent application of cybersecurity principles to ensure a safe, efficient, and reliable educational process. Cybersecurity in the educational context is not only about protecting personal data but also encompasses the stability of the digital infrastructure that supports online learning systems. The OECD (2023) emphasizes that educational institutions need to build a digital resilience framework that integrates risk management, data protection policies, and security training for all stakeholders. The reliability of online learning systems depends heavily on the institution's ability to prevent, detect, and respond to cyber incidents quickly and appropriately. Failure in this area can lead to significant disruptions to the learning process, loss of public trust, and even the loss of academic data that is difficult to recover. Therefore, strengthening cybersecurity literacy needs to be aligned with the development of technological infrastructure so that digital education systems are not only technically sophisticated but also ethically and functionally robust. The synergy between cybersecurity policies and a culture of digital literacy will create a safe and sustainable learning environment in the digital education era.

The involvement of the entire education ecosystem—including the government, schools, parents, and the community—is a prerequisite for the success of cybersecurity-oriented digital literacy. The government needs to provide regulations and policies that support the integration of digital security into education, while schools play a role as implementers and developers of best practices on the ground. Parental and community support is also crucial to ensure the consistency of digital security values beyond the school environment. This kind of multi-sector collaboration reflects a whole-of-society approach, where cybersecurity awareness is viewed as a social responsibility, not simply a technical obligation. Furthermore, partnerships with technology institutions and digital security communities can enrich the curriculum and provide contextual and up-to-date learning resources. When all parties are actively involved, digital literacy and cybersecurity become not just training programs but also a collective culture embedded in educational life. Such an ecosystem will strengthen the resilience of national education against global digital threats while increasing public trust in technology-based learning systems.

The future success of hybrid and virtual education will largely depend on the education system's ability to strike a balance between digital innovation and cybersecurity protection. Strong digital literacy will foster teachers' and students' ability to creatively adapt to new technologies, while cybersecurity awareness will ensure that innovation occurs ethically and safely. Sustainable education requires a holistic approach

that combines the cognitive, technological, and moral dimensions of digital technology use. If this awareness is deeply internalized, education in the digital era will not only produce individuals who are proficient in using technology but also digital citizens who are responsible and resilient to global challenges. The application of digital literacy principles integrated with cybersecurity will strengthen the foundation of ethics and professionalism in education. Thus, the future of digital education can develop inclusively, adaptively, and sustainably without sacrificing the security and humanitarian values that are at the heart of the learning process itself..

## METHODS

The research method used in the study entitled "Digital Literacy and Cybersecurity for Teachers and Students in the Era of Hybrid and Virtual Education" utilizes a qualitative approach with a literature review study design. This approach was chosen because the study aims to deeply explore phenomena, concepts, and theoretical constructs related to digital literacy and cybersecurity in the realm of modern education. Qualitative research allows researchers to understand the meaning and social context of various relevant literature without manipulating variables. According to Creswell (2018), qualitative research aims to interpret the meaning of social and cultural experiences studied through non-numerical data sources, including scientific texts, reports, and policy documents. Thus, this approach provides space for reflective analysis of the relationship between digital literacy, cybersecurity competencies, and the dynamics of hybrid learning that are rapidly developing in the era of digital transformation.

The type of research used is a systematic literature review study, a method that focuses on the collection, evaluation, and synthesis of previous research results in a structured manner to gain a comprehensive understanding of a scientific topic. Snyder (2019) explains that a literature review study serves to map concepts, assess research gaps, and identify trends and theoretical implications of various previous studies. Through this technique, researchers can explore how digital literacy and cybersecurity are positioned in the context of hybrid education and find the most relevant conceptual model for strengthening the capacity of teachers and students. This research not only compiles study results but also interprets their interrelationships within a broader conceptual framework, resulting in a synthetic and argumentative academic contribution.

The research procedure was carried out through several systematic stages, starting with topic identification and problem formulation, followed by literature collection, source selection and evaluation, content analysis, and conceptual synthesis. The primary data sources were scientific journal articles, reports from UNESCO, the OECD, and the European Commission, as well as academic literature published between 2015 and 2025 that were relevant to the research theme. The literature selection process was conducted using the principles of inclusion and exclusion to ensure the relevance and validity of the sources. Only studies containing variables or concepts related to digital literacy, cybersecurity, and hybrid and virtual education practices were included in the analysis. The content analysis stage was conducted thematically to identify patterns, trends, and relationships between concepts from previous research. This analysis technique followed the guidelines of Krippendorff (2019), which emphasizes the importance of interpreting symbolic meanings in scientific texts to produce in-depth and contextual findings.

The collected data were then categorized based on the main themes, namely: (1) digital literacy for teachers and students, (2) cybersecurity in educational environments, (3) digital policies and curricula, and (4) strategies for strengthening digital competencies in hybrid systems. This grouping facilitates researchers to explore the

conceptual relationship between digital literacy and cybersecurity as two complementary dimensions in the digital learning ecosystem. Each category was analyzed by considering theoretical and empirical perspectives from various sources to build a holistic conceptual framework. Miles, Huberman, and Saldaña (2014) emphasized that qualitative analysis needs to involve an iterative process of data reduction, data presentation, and conclusion drawing to produce reliable findings. Thus, this study produces a scientific synthesis that is not only descriptive, but also interpretive of the dynamics of digital security in educational environments.

To clarify the methodological stages, the following table presents the literature review research flow used in this study:

| Research Stages | Activity Description | Expected Output |
|---|---|---|
| **Topic Identification and Problem Formulation** | Determining the research focus on digital literacy and cybersecurity in hybrid education | Formulation of problems and research objectives that are focused |
| **Literature Collection** | Collecting scientific sources from journals, policy reports, and academic publications 2015–2025 | Relevant and valid literature corpus |
| **Selection and Evaluation of Sources** | Selecting based on inclusion criteria (relevant, up-to-date, peer-reviewed) | List of literature worthy of analysis |
| **Content Analysis (Content Analysis)** | Identify themes, patterns, and relationships between concepts in literature | Categories and thematic patterns of research |
| **Synthesis and Conclusion Drawing** | Develop a conceptual interpretation that explains the integration of digital literacy and cybersecurity | Conceptual model and theoretical implications |

The analysis process was conducted using a thematic synthesis approach, where each literature was reviewed to identify consistent conceptual threads across studies. This approach allows for in-depth exploration of issues such as teachers' digital competency gaps, cybersecurity challenges in schools, and strategies for integrating digital literacy into national education policy. According to Thomas and Harden (2008), thematic synthesis is effectively used to connect empirical findings with broader theoretical constructs, thereby producing a new synthesis relevant to the development of educational policy and practice. The final result of this process is a conceptual model that illustrates the interrelationships between digital literacy, cybersecurity, and the effectiveness of hybrid learning.

The credibility of the research results was maintained through conceptual validation and source triangulation, comparing findings from various academic literatures from different disciplines such as education, information technology, and digital psychology. Lincoln and Guba (1985) emphasized that the validity of qualitative research can be achieved through four main criteria: credibility, transferability, dependability, and confirmability. In this study, credibility was strengthened by selecting literature from reputable international journals, while transferability was maintained by detailing the context of hybrid education so that the study results could be applied to similar situations. Dependability was achieved by systematically documenting the analysis steps, and confirmability was maintained through critical reflection on the researcher's position in interpreting the data. Thus, this study meets the standards of methodological rigor and is scientifically accountable.

The results of this literature review are expected to provide a comprehensive mapping of the challenges and opportunities for integrating digital literacy and cybersecurity in the era of hybrid and virtual education. This study not only presents a conceptual synthesis of various studies but also offers a theoretical basis for developing educational policies oriented towards digital security and sustainability. Through a reflective and analytical qualitative approach, this research makes a scientific contribution to strengthening the capacity of teachers and students to navigate the complexities of the digital world. The findings are expected to serve as a foundation for further, more empirical research and strategic guidance for educational institutions in building a digital learning ecosystem that is intelligent, ethical, and cybersafe.

## RESULTS AND DISCUSSION

### 1. Digital Literacy as the Foundation of Teacher and Student Competence in Hybrid and Virtual Learning

The development of information technology has given rise to legal and social transformations that require a redefinition of citizens' rights and obligations in accessing and using digital resources. In the context of education, digital literacy serves as a legal and pedagogical instrument to guarantee the implementation of the right to quality education as guaranteed in Article 31 of the 1945 Constitution. Digital literacy for teachers and students is not only a technical competency, but also part of the right to education in the digital era, which emphasizes the ability to understand, select, and use information responsibly. The inability to understand digital literacy implies a violation of the principle of due diligence in the safe and ethical use of educational technology. Therefore, educational institutions are obliged to enforce internal policies that align with the principle of digital prudence as reflected in norms on personal data protection and intellectual property rights.

The application of digital literacy in hybrid and virtual education reflects the state's responsibility to ensure equal access to technology-based education. Teachers hold a strategic legal position as implementers of public policy in the education sector, thus requiring digital competencies regulated through continuous professional development mechanisms. Legal instruments such as the Freedom to Learn Policy and the 2021 Ministry of Education, Culture, Research, and Technology Digital Transformation Roadmap serve as the normative umbrella governing the implementation of digital-based learning. Meanwhile, students, as subjects of learning, have the right to protection from the risk of digital data misuse during online learning. Therefore, improving digital literacy is not only a pedagogical effort but also a form of fulfilling the state's legal obligation to protect students from digital inequality and cyber exploitation.

The concept of digital literacy is also closely linked to the principles of accountability and transparency in the education system. Teachers, as key actors in online learning, must understand digital public ethics to avoid violating the principles of openness and data protection stipulated in Law Number 27 of 2022 concerning Personal Data Protection. The use of learning technologies such as Learning Management Systems (LMS) and cloud storage must comply with legal principles of consent and purpose limitation in managing student data. Failure to comply with these principles can result in both administrative and civil legal liability. Thus, digital literacy serves a dual function as an educational tool and legal protection in the use of educational technology.

Theoretically, digital literacy should be viewed as part of digital legal competency, encompassing awareness of rights and obligations within the educational cyberspace.

Strengthening digital literacy means upholding the principle of legal awareness among teachers and students so they can use technology in accordance with applicable legal norms. Legal institutions in digital education not only protect individual interests but also ensure the continuity of a national education system with integrity. Neglecting digital literacy is tantamount to neglecting the professional responsibilities stipulated in the educator's code of ethics. Therefore, developing digital literacy is an integral part of digital educational governance, which ensures a balance between academic freedom and legal compliance.

Thus, digital literacy in hybrid and virtual learning serves as a regulatory and protective mechanism against the misuse of technology in education. Teachers and students are required not only to act as users but also as subjects of digital law, aware of the legal implications of every online action. Digital literacy shapes legal behavior based on technological ethics, strengthens a culture of compliance, and fosters a sense of collective responsibility for the security and integrity of the learning process. Overall, digital literacy serves as the legal foundation for adaptive, democratic, and equitable education amidst social changes brought about by the digital revolution.

## 2. Cybersecurity as a Pillar of Erhnics and Data Protection in the Digital Education Ecosystem

Cybersecurity in education holds a fundamental position as a form of legal protection for the privacy and information security rights of students and educators. From a public law perspective, the state has a constitutional obligation to protect its citizens from digital threats, as stipulated in Article 28G of the 1945 Constitution, which guarantees the right to a sense of security. Therefore, cybersecurity in the education sector must be understood as part of cyber law, which functions to protect the public interest against crimes or misuse of electronic systems. National regulations such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions serve as the legal basis for education providers in securing digital data. Implementation of these laws requires educational institutions to have adequate and standardized digital security governance.

Cybersecurity is also closely related to the duty of care principle inherent in the teaching profession as managers of students' personal data. Teachers and schools have a legal responsibility to ensure that all online learning activities do not result in privacy violations or misuse of personal information. If data leaks occur due to security system negligence, administrative or even criminal liability may arise. Therefore, every educational institution is required to have a cybersecurity Standard Operating Procedure (SOP) that complies with laws and regulations. Furthermore, students must also be provided with digital legal awareness education to understand their rights in cyberspace, including the right to be protected from data exploitation and online violence.

Digital ethics serves as both a moral and legal foundation for implementing cybersecurity in education. The principles of non-maleficence (doing no harm to others) and autonomy (respect for privacy rights) must be applied in every digital interaction between teachers and students. Education that fails to internalize digital ethics risks giving rise to legal violations, whether in the form of plagiarism, data theft, or information manipulation. According to Solove (2021), strengthening digital ethics in educational institutions is a preventative strategy to prevent legal violations in cyberspace. Thus, cybersecurity is not merely technical but also contains a normative dimension that binds every digital citizen to act in accordance with the law and public morality.

From a governance perspective, cybersecurity must be integrated into public administration law-based education management systems. Educational institutions are required to develop internal policies that regulate responsibilities, data protection mechanisms, and sanctions for digital security violations. This approach aligns with the principles of good governance, which prioritize accountability, transparency, and fairness in all administrative actions. Oversight can be carried out through regular digital security audits and evaluations of compliance with international standards such as ISO/IEC 27001 on information security management. Through these mechanisms, digital education is not only technologically efficient but also legally and ethically sound.

Cybersecurity in education must ultimately be viewed as a legal pillar supporting the sustainability of digital learning systems. Teachers and students, as part of the digital society, need to be equipped with a strong understanding of the law and ethical awareness to navigate cyber risks responsibly. Cybersecurity is not only about preventing threats but also about maintaining legal trust between education providers and students. Therefore, digital education policy reform must prioritize cybersecurity as a normative priority in the implementation of technology-based learning.

## 3. Integration of Digital Literacy and Cybersecurity in Continuing Education Policies and Curricula

The integration of digital literacy and cybersecurity into education policy is an urgent legal necessity given the increasing dependence of education on technology. This integration principle aligns with Article 12 of Law Number 20 of 2003 concerning the National Education System, which affirms that students have the right to receive education that is relevant to current developments. This means that the state has a legal obligation to ensure that the national curriculum prepares students to face the challenges of the digital era. Within the legal framework of educational administration, regulations regarding digital literacy and cybersecurity must be institutionalized through ministerial regulations, technical guidelines, and national education standards. In this way, digital policy will not be sporadic but rather become a measurable and sustainable regulatory system.

The integration of digital literacy and cybersecurity policies also needs to consider the principle of lex specialis derogat legi generali, where digital education policies must have a specific legal basis that complements general regulations on information technology. The government can issue derivative regulations in the form of a Minister of Education Regulation on Cybersecurity Governance and Digital Literacy in Schools and Universities. This legal instrument can regulate digital competency standards for teachers, cyber training mechanisms, and educational institutions' obligations to protect academic data. Thus, digital education policies are not only normative but also operational and legally enforceable. This approach strengthens the rule of law in digital education and emphasizes the state's responsibility to create a cybersafe learning environment.

From a curriculum perspective, the integration of digital literacy and cybersecurity must be realized through a revised curriculum that incorporates digital education as a core cross-disciplinary competency. Teachers need to be given legally based pedagogical authority to instill digital security values starting from elementary school. Such a curriculum serves as a preventative legal education tool to protect the younger generation from the risk of cyber law violations. Furthermore, digital security education needs to be synergized with character education to foster legal awareness and public morality in cyberspace. Thus, the curriculum not only transfers technological knowledge but also instills sustainable digital legal discipline.

This integration policy also requires ongoing legal oversight and evaluation to ensure its implementation does not stop at the administrative level. Oversight bodies such as the Inspectorate General and the Public Information Commission can play a role in ensuring that every educational institution adheres to the principles of digital transparency, security, and accountability. Furthermore, partnerships with independent institutions such as the National Cyber and Crypto Agency (BSSN) can strengthen schools' capacity to professionally manage cyber threats. This collaboration reflects the application of the principle of cooperative governance in modern administrative law, where the state, society, and the private sector play a joint role in protecting the public interest in the digital world.

By integrating digital literacy and cybersecurity into sustainable education policies, the national education system will have strong legal legitimacy in facing the era of global digitalization. This approach ensures that technological transformation in education is aligned with legal principles, ethics, and social justice. Legally regulated digital education will guarantee the protection of students' rights, strengthen teacher professionalism, and enhance the nation's competitiveness internationally. Thus, the law serves not only as a regulatory instrument but also as a philosophical foundation that affirms digital education as a fundamental right and a shared responsibility in building a civilized cyber society.

## CONCLUSIONS

The conclusion of the study on digital literacy and cybersecurity for teachers and students in the era of hybrid and virtual education confirms that technology-based educational transformation requires not only technical adaptability but also the importance of legal protection and digital ethics as an integral part of the right to a safe and dignified education. Digital literacy serves as a juridical-philosophical foundation for realizing responsible freedom of learning, where every individual has the capacity to access, process, and utilize information critically without violating applicable legal norms. Mastery of cybersecurity is a form of self-protection as well as a legal obligation to maintain the confidentiality of personal data and prevent digital violations that could potentially harm others. Teachers, as legal subjects in the education system, are obliged to ensure the use of learning technology complies with the principles of digital prudence stipulated in laws and regulations regarding data protection and intellectual property rights. Meanwhile, students have the right to digital protection as well as the legal responsibility to maintain ethical interactions in cyberspace. The integration of digital literacy and cybersecurity must be positioned as a sustainable education policy oriented towards law enforcement, academic ethics, and the protection of students' personal data. This legal affirmation requires synergy between educational institutions, the government, and national cyber authorities to develop regulations that adapt to developments in digital technology. Establishing a responsive legal framework will strengthen legal certainty for all educational actors in facing the challenges of digital globalization. Furthermore, digital legal awareness needs to be instilled through formal curricula and professional training that is preventative, not merely reactive to violations. Education grounded in digital literacy and cybersecurity will create a learning ecosystem that is transparent, accountable, and digitally just. Therefore, the success of education in the hybrid and virtual era is crucially determined by collaboration between stakeholders in upholding the principles of legality, digital ethics, and data protection, oriented toward universal humanitarian values.

## REFERENCE

Buchan, M. C., & kolega (2024). *Practical activities and curriculum design to teach cybersecurity concepts to K-12: Case studies and toolkit.* Computers in Human Behavior Reports, 2024. https://doi.org/10.1016/j.chbr.2024.100501

Buchan, M. C., et al. (2024). *An evidence-based framework for digital literacy interventions in schools.* Smart Learning Environments / related special issue. https://doi.org/10.1186/s40561-024-00293-x

Buchan, M. C., et al. (2024). *Development of an evidence-based digital literacy program to support digital learning.* Smart Learning Environments, 11, Article 29. https://doi.org/10.1186/s40561-024-00293-x

Buchan, M. C., Pérez-Escoda, A., & kolega (2024). *Evidence and best practices for integrating cybersecurity awareness in hybrid classrooms.* Smart Learning Environments / Education journals, 2024. https://doi.org/10.1186/s40561-024-00293-x.

Childers, G., Linsky, C. L., Payne, B. R., Byers, J., & Baker, D. (2023). *K-12 educators' self-confidence in designing and implementing cybersecurity lessons.* Computers & Education Open, 4, 100119. https://doi.org/10.1016/j.caeo.2022.100119

Deschênes, A. A. (2023). *Digital literacy, the use of collaborative technologies, and perceived social proximity in a hybrid work/education environment.* Computers in Human Behavior Reports, 13, Article 100351. https://doi.org/10.1016/j.chbr.2023.100351

Ebrahimi, E. (2025). *A review of current cybersecurity education for young learners: Curriculum and pedagogy.* (ScitePress).

Fouad, N. S., et al. (2021). *Securing higher education against cyberthreats.* Journal of Cybersecurity/Policy (special issue), 2021. https://doi.org/10.1080/23738871.2021.1973526

Gómez-Puerta, M., & Chiner, E. (2024). *Teachers' perceptions on online behaviour and risk mediation: Implications for cybersecurity education.* International Journal for Child–Computer Interaction (review & articles), 2024.

Gómez-Puerta, M., Chiner, E., Villegas-Castrillo, E., & Suriá-Martínez, R. (2024). *Digital and mediation competence for students' safe use of the Internet: Enhancing teacher training.* Education Sciences, 14(12), 1399. https://doi.org/10.3390/educsci14121399

Guillén-Gámez, F. D., Martínez-García, I., & kolega (2024). *Digital competences in cybersecurity of teachers in training.* Computers in the Schools, 41(3), 281–306. https://doi.org/10.1080/07380569.2024.2361614

Guillén-Gámez, F. D., Tomczyk, Ł., Ruiz-Palmero, J., & Connolly, C. (2024). *Digital security in educational contexts: Digital competence and challenges for good practice.* Computers in the Schools, 41(3), 257–262. https://doi.org/10.1080/07380569.2024.2390319.

Ismail, M., Madathil, N. T., Alalawi, M., Alrabaee, S., Al Bataineh, M., Melhem, S., & Mouheb, D. (2024). *Cybersecurity activities for education and curriculum design: A survey.* Computers in Human Behavior Reports, 16, Article 100501. https://doi.org/10.1016/j.chbr.2024.100501

Manganello, F., Earp, J., Fante, C., Bassi, G., Fabbri, S., Matteucci, I., Vaccarelli, A., Olesen, N., de Vibraye, A., Callaghan, P., & Gentile, M. (2024). *Shaping the foundation of the SuperCyberKids Learning Framework: A comprehensive analysis of cybersecurity education initiatives.* Frontiers in Education, 9, Article 1375853. https://doi.org/10.3389/feduc.2024.1375853.

Perifanou, M., & Economides, A. A. (2023). *Assessing teachers' digital competence in primary and secondary education: Applying a new instrument to integrate pedagogical*

*and professional elements for digital education.* Education and Information Technologies. https://doi.org/10.1007/s10639-023-11848-9.

Prümmer, J., van Steen, T., & van den Berg, B. (2024). *A systematic review of current cybersecurity training methods.* Computers & Security, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585

Sağlam, R. B., Miller, V., & Franqueira, V. N. L. (2023). *A systematic literature review on cyber security education for children.* IEEE Transactions on Education, 66, 274–286. https://doi.org/10.1109/TE.2022.3231019.

Sánchez-Cruzado, C., Santiago Campión, R., & Sánchez-Compaña, M. T. (2021). *Teacher digital literacy: The indisputable challenge after COVID-19.* Sustainability, 13(4), 1858. https://doi.org/10.3390/su13041858

Torres-Hernández, N., & Gallego-Arrufat, M.-J. (2022). *Indicators to assess preservice teachers' digital competence in security: A systematic review.* Education and Information Technologies, 27, 8583–8602. https://doi.org/10.1007/s10639-022-10978-w.

Walsh, K., Wallace, E., Ayling, N., & Sondergeld, A. (2022). *Best practice framework for online safety education: Results from a rapid review, expert review and stakeholder consultation.* International Journal of Child–Computer Interaction, Article 100474. https://doi.org/10.1016/j.ijcci.2022.100474.

.