

CENTRAL ASIAN JOURNAL OF LITERATURE, PHILOSOPHY, AND CULTURE

https://cajlpc.centralasianstudies.org/index.php/CAJLPC

Volume: 07 Issue: 04 | October 2026 ISSN: 2660-6828

Article

From Framework to Practice: Integrating the 4Cs Online Risk Model and Operational Digital Security Components in First-Year Digital Literacy Education

Kautsarina[1], Yolanda Presiana Desi[2], Fahrizal Lukman Budiono[3]

1. Ministry of Communication and Digital Affairs, Jakarta, Indonesia
2. Sekolah Tinggi Multi Media, Yogyakarta, Indonesia
3. Ministry of Communication and Digital Affairs, Jakarta, Indonesia

* Correspondence: kaut001@komdigi.go.id[1], yolanda@mmtc.ac.id[2], fahr004@komdigi.go.id[3]

Abstract. Despite widespread adoption of the 4Cs framework in online safety policy, its operational translation into classroom digital security practices remains limited. This study investigates the integration of the 4Cs online-risk framework (Content, Contact, Conduct, and Commerce/Contract) with four operational digital security components (privacy protection, content ethics, device security, and critical literacy) to enhance digital literacy and safety awareness among first-year university students. Data were collected through observation, group worksheets, and reflective reports. Results indicate that students demonstrated enhanced critical awareness of digital safety, were able to connect theoretical frameworks to real-world issues, and developed creative communication outputs. This approach contributes to the pedagogical model of digital literacy by linking theoretical and operational perspectives, fostering ethical digital conduct and awareness of online risks. Early implementation is strategically chosen to shape students' foundational digital behaviours and critical judgment during the formative stage of academic socialisation, amplifying long-term and community impact of safe digital practices. Using a case-based learning approach, three student groups per class analysed real-world digital safety cases and produced infographics as awareness artefacts. Findings demonstrate that first-year learners can meaningfully apply theoretical risk models to operational actions, develop ethical reflection, and communicate safety messages effectively. Thus, students demonstrated not only comprehension but measurable improvement in digital safety awareness and ethical reasoning. The distinctiveness of this research lies in creating a pedagogical model that bridges the 4C taxonomy (policy-oriented) with a competence-based operational framework relevant to DigComp 2.2. This replicable model uniquely links theory, practice and public awareness. The findings align with recent studies supporting contextualised and creative digital-literacy approaches. Overall, this model offers a promising pathway to foster ethical, privacy-conscious digital citizens and strengthen digital resilience within higher education and society at large.

Keywords: Digital Awareness, Digital Literacy, Digital Safety, Higher Education, Online Risk

Citation: Kautsarina. From Framework to Practice: Integrating the 4Cs Online Risk Model and Operational Digital Security Components in First-Year Digital Literacy Education. Central Asian Journal of Literature, Philosophy, and Culture 2026, 7(4), 68-74.

Received: 10th Apr 2026
Revised: 11th May 2026
Accepted: 28th Jun 2026
Published: 20th Sep 2026

Copyright: © 2026 by the authors. Submitted for open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

Introduction

The acceleration of digital innovation has reshaped the learning landscape in higher education, influencing how students communicate, access knowledge, and participate in online communities. Yet, increased dependence on digital spaces inevitably heightens vulnerability to online threats such as disinformation, financial fraud, cyberbullying, and breaches of personal data. Consequently, universities must reinforce students' digital literacy and awareness of online safety as part of core learning expectations. First-year students represent a particularly at-risk group during their transition from structured secondary schooling to more independent digital engagement, often lacking sufficient ability to recognise manipulation, data exploitation, or unsafe online behaviours[1]

This paper introduces a pedagogical approach that combines the 4Cs framework for online risk, originating from the EU Kids Online initiative[2], with four practical dimensions of digital security: (1) privacy and personal data management, (2) ethical participation in online spaces, (3) security of devices and user accounts, and (4) critical assessment of digital information. The model aims to connect conceptual digital-literacy frameworks to concrete security skills through experiential learning designed for first-year university students. Embedding this structured learning early in students' academic experience is intended to cultivate responsible judgement and foundational digital practices, supporting a culture of secure, reflective, and ethical digital behaviour within and beyond higher education.

Literature Review

This section consolidates three key domains: the 4Cs model of online risk, operational elements of digital-security behaviour, and the pedagogical role of information graphics as learning artefacts. Integrating these perspectives provides the theoretical grounding for an experiential intervention that promotes awareness, critical thinking, and safer online practices.

The 4Cs Framework of Online Risk

The 4Cs framework categorises major online threats faced by children and young people, developed through the EU Kids Online research and further progressed by the CO:RE programme[2], [3]. Content risks relate to exposure to harmful or inappropriate material, such as violent imagery, misinformation, disinformation, hate content, or clickbait. Contact risks occur when individuals are engaged by strangers or harmful actors in digital communication spaces. Conduct risks concern behaviour that causes harm to oneself or others, such as harassment, bullying, and irresponsible sharing of personal material. Contract/Commerce risks relate to exploitation or deception linked to digital transactions or commercial activities. A recent comparative review by Jang & Ko across Australia, Canada, and the UK demonstrated that while the 4Cs framework is widely adopted in safety policy, its direct educational application remains underutilised[4].

Operational Digital Security Components

The 4Cs model may be connected to four practice-oriented security capacities:

1. Privacy and Data Protection refers to the ability to manage, protect, and understand the use of personal information in online interactions [5], [6].

2. Ethical Online Behaviour refers to responsible participation grounded in respect, legal awareness, platform norms, and acknowledgement of consequences of digital actions [7].

3. Device and Account Security refers to practical cyber-hygiene involving strong authentication, update management, and phishing prevention[8].

4. Critical and Reflective Digital Literacy refers to the capacity to evaluate credibility, bias, accuracy, and intent within digital content, supporting informed and safe decision-making[9].

Within the European DigComp 2.2 framework, the Safety competence area emphasises protection of personal data, devices, and digital well-being [10], [11], aligning closely with the operational structure adopted in this study.

Information Graphic in Pedagogy

An information graphic, commonly known as an infographic, is a visual communication tool designed to translate complex or data-rich information into clear, accessible, and engaging visual representations [12] By integrating text, imagery, data visualisation, and design elements, infographics facilitate more effective cognitive processing, enabling learners to understand and internalise key concepts more efficiently than through text alone. This visual structuring supports improved learning outcomes,

memory retention, and long-term recall, which are essential foundations for encouraging changes in attitudes and behaviours.

In recent years, infographics have gained significant prominence as a digital medium for disseminating knowledge, particularly in contexts where information is dense, abstract, or needs to reach audiences from diverse literacy levels and backgrounds [13]. Their concise yet impactful format allows creators to convey essential messages with clarity, accuracy, and persuasive power, making them an increasingly preferred strategy in education, public communication, and awareness-raising initiatives [14].

2. Methodology

2.1 Pedagogical Model

Case-based learning is the use of case-based approach that engages students in discussing specific situations and real-world examples. This method is student-centered and involves intensive interaction among discussion participants. Case-based learning is an instructional method designed to enhance higher-order thinking in solving a case. It helps students connect education with specialized training while developing professional skills for practice [15]. The proposed model (Figure 1) positions the 4Cs as a framework for analysing real digital-risk cases while mapping identified risks to operational security components through collaborative case-based learning.

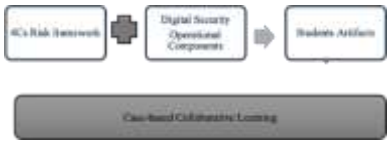


Figure 1. Pedagogical Model Integrating the 4Cs Digital-Risk Framework with Digital-Security Operational Components through a Case-Based Collaborative Learning Approach

First-year students often lack prior technical knowledge and disciplinary experience. Case-based collaborative learning (CBCL) addresses these challenges through several instructional strategies i.e. 1) Scaffolding: Lectures provide short targeted introductions to each domain and case context, 2) Decoupling technical complexity: This lowers cognitive barriers while maintaining the essence of the analytical skill being taught, 3) Collaborative learning studies: This helps novices build confidence and competence as they navigate unfamiliar content. Together, these strategies reflect an adaptive, learner-responsive approach that supports first-year students' transition into university-level problem-solving while maintaining high expectations for engagement and intellectual challenge [16].

2.2 Research Context and Participants

The research was implemented in a first-semester Digital Literacy course at a university in Yogyakarta, Indonesia, during the 2025–2026 academic year. Early intervention is strategically important because first-year students face unfamiliar freedoms and emerging risk behaviours[17]. Participants were organised into 12 groups drawn from four classes.

2.3 Procedure

To evaluate the learning outcomes produced through the case-based collaborative design process, a total of 24 infographics were analysed across 12 student groups, with each group completing two infographic artefacts derived from six distinct real-world digital risk cases. The assessment was conducted using the multidimensional rubric(see Table 1), encompassing conceptual understanding of the 4Cs model, application of operational digital security components, ethical reflection, collaborative contribution, and communication design quality. Authentic case-based learning enables students to connect

theoretical risk models to practical, lived challenges and encourages transferable cybersecurity habits. Working with a structured worksheet, students first classified risks according to the 4Cs and then mapped them to corresponding operational components. Groups subsequently developed infographics using digital design tools such as Canva or PowerPoint to communicate preventive strategies and public-facing messages[14], transforming students into knowledge disseminators[18], [19]. Data sources included worksheets, infographics, and instructor observation.

2.4 Assessment Rubric

The evaluation rubric (Table 1) assessed conceptual accuracy, ethical reasoning, teamwork, and quality of communication, dimensions aligned with authentic performance-based learning in cybersecurity education.

2.5 Data Analysis

A triangulated qualitative approach was employed to strengthen the credibility of the analysis. The worksheets produced by student groups were examined and coded to verify the accuracy of risk categorisation and the alignment of these risks with relevant operational security components. Meanwhile, individual reflective essays were subjected to thematic analysis to capture evidence of ethical sensitivity, emotional engagement, and indicators of perceived behavioural shifts [20]. In addition, the infographic outputs were reviewed to assess the clarity of message delivery, the coherence of issue framing, and the practicality of the recommended preventive measures[13], [14].

Table 1. Assessment Rubric for Digital-Safety Learning Artefacts.

Criterion	Excellent (4)	Good (3)	atisfactory (2)	ed Improvement (1)
Conceptual understanding of 4Cs	Fully accurate classification of risks for the case	Mostly accurate classification, minor errors	Some misclassification or omissions	Incorrect or missing classification
Application of operational components	Clear, appropriate mapping from risks to components	Good mapping, some minor mismatches	Acceptable mapping, but incomplete	Poor or no mapping to operational components
Ethical reflection	Insightful, personal, connects behaviour and values	Good reflection, includes some personal insight	Basic reflection, limited critical perspective	Minimal or no reflection
Collaboration	All members contribute, and strong teamwork is evident	Good teamwork, minor imbalance	Some group imbalance, uneven contribution	Poor teamwork, one or fewer participants

Creativity and communication in infographic	Highly engaging design, clear message, accurate recommendations	Good design, message clear, minor layout issues	Usable design, message moderately clear	Unclear message, poor design quality

3. Result and Discussion

3.1 Learning Outcomes

Results showed that student groups successfully identified multiple digital risks using the 4Cs model. For example, in the phishing case group, students noted Contact risks (fraudulent communication), Contract/Commerce risks (financial exploitation), and Content risks (malicious link). They then linked these to operational components: privacy/data protection (secure credentials), device/system security (software update and phishing awareness). Students articulated these mappings in worksheets and highlighted them in their infographics.

Collaborative learning enhanced peer-awareness and digital empathy. The peer-group discussions revealed that students recognised how their own device habits could expose others, and how digital behaviour can have broader social ramifications.

3.2 Infographic as a Learning Artefact

Infographics are one of the more interesting modes of presenting information visually through diagrams, videos, charts, text images, and the like [21]. Infographics enabled students to transform theoretical understanding into communicable safety campaigns. The outputs included persuasive statistics, behaviour-based recommendations, and visual metaphors that linked risk types with daily digital habits (Figure 2). Among the 24 infographics, 75% achieved a Good to Excellent range based on the rubric, indicating successful transition from comprehension to competent real-world application of security concepts. This study contributes a unique model that connects theoretical risk frameworks with operational cybersecurity practices through authentic artefact-based assessment, an approach not frequently documented in existing literature.



Figure 2. Sample of infographics created by students (in Bahasa Indonesia)

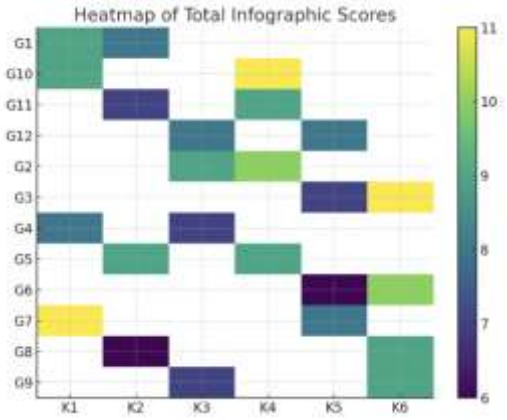


Figure 3. Heatmap of Total Infographic Scores

Figureure 3 presents a heatmap visualisation of total scores across 24 infographic artefacts. The column dimension represents six cybersecurity case contexts (K1–K6), while rows correspond to 12 student groups (G1–G12). Higher intensity values indicate stronger performance. A visible clustering around phishing (K1) and ransomware (K6) suggests greater conceptual accessibility, whereas weaker activity patterns in privacy leakage (K5) reflect gaps in practical solution articulation. This reinforces prior observations that topic familiarity significantly influences analytical depth and preventive strategy development.

3.3 Educational Implications

The results confirm that combining conceptual frameworks with practical application strengthens holistic digital safety competence. Echoing the broader literature, instruction that centres on authentic, real-world problems consistently appears to strengthen students' analytic capacities and engagement within cybersecurity education. Practical, hands-on projects and narrative scenarios help learners practise decision-making under realistic constraints and foster collaborative problem solving [22]. Implementing the model early in university creates sustainable digital habits and supports wider community awareness through public-facing artefacts. Alignment with DigComp 2.2 offers a structured basis for curriculum enhancement [11].

3.4 Limitations and Further Research

Limitations include a small sample, single-institution context, and short-term evaluation. Future research should examine long-term behavioural transformation, incorporate quantitative assessment, expand to other disciplines, and adapt for online or hybrid delivery.

4. Conclusion

The integration of the 4Cs framework with operational security competencies offers an effective pedagogical strategy for improving students' digital-safety awareness. Through collaborative authentic learning, students developed the ability to identify online threats and apply preventive actions responsibly. The novelty of this research lies in its structured connection between conceptual policy-level frameworks and actionable skills aligned with DigComp 2.2, producing a model that is adaptable and replicable across higher-education settings. Early adoption supports ethical, privacy-conscious digital citizenship and reinforces institutional digital resilience.

References:

[1] G. Öncül, "Defining the need: digital literacy skills for first-year university students," Journal of Applied Research in Higher Education, vol. 13, no. 4, pp. 925–943, Dec. 2020, doi: 10.1108/JARHE-06-2020-0179.

[2] S., Livingstone and M. Stoilova, "The 4Cs: Classifying Online Risk to Children," Hamburg, 2021. doi: 10.21241/ssoar.71817.

[3] M. Stoilova, M. Rahali, and S. , Livingstone, "Classifying and responding to online risk to children Good practice guide," London, Feb. 2023.

[4] Y. Jang and B. Ko, "Online Safety for Children and Youth under the 4Cs Framework—A Focus on Digital Policies in Australia, Canada, and the UK," Children, vol. 10, no. 8, 2023, doi: 10.3390/children10081415.

[5] Snježana Stanarević Katavić, Hajdi Ivanović, and Anita Papić, "Digital privacy and data protection knowledge and skills of university students in Croatia: Preliminary findings," Education for Information, vol. 39, no. 4, pp. 493–515, Nov. 2023, doi: 10.3233/EFI-230056.

[6] R. Iskandar, A. Maksum, and A. Marini, "Digital citizenship literacy in Indonesia: The role of privacy awareness and social campaigns," Social Sciences and Humanities Open, vol. 12, Jan. 2025, doi: 10.1016/j.ssaho.2025.101697.

[7] I. Isabella, A. Alfitri, A. Saptawan, N. Nengyanti, and T. Baharuddin, "Empowering Digital Citizenship in Indonesia: Navigating Urgent Digital Literacy Challenges for Effective Digital Governance," Journal of Governance and Public Policy, vol. 11, no. 2, pp. 142–155, Jun. 2024, doi: 10.18196/jgpp.v11i2.19258.

[8] F. D. Guillén-Gámez, Ł. Tomczyk, J. Ruiz-Palmero, and C. Connolly, "Digital Security in Educational Contexts: Digital Competence and Challenges for Good Practice," 2024, Routledge. doi: 10.1080/07380569.2024.2390319.

[9] A. Wichita Putri Hariyanto and aini Perdani, "Understanding Students' Digital Literacy as Part of Their Personal Information Management Skills."

[10] L. Van Audenhove, L. Vermeire, W. Van den Broeck, and A. Demeulenaere, "Data literacy in the new EU DigComp 2.2 framework how DigComp defines competences on artificial intelligence, internet of things and data," Information and Learning Sciences, vol. 125, no. 5–6, pp. 406–436, Feb. 2024, doi: 10.1108/ILS-06-2023-0072.

[11] Riina. Vuorikari, Stefano. Kluzer, and Yves. Punie, DigComp 2.2, The Digital Competence framework for citizens : with new examples of knowledge, skills and attitudes. Publications Office of the European Union, 2022.

[12] L. Traboco, H. Pandian, E. Nikiphorou, and L. Gupta, "Designing Infographics: Visual Representations for Enhancing Education, Communication, and Scientific Research," J Korean Med Sci, vol. 37, no. 27, 2022, doi: 10.3346/jkms.2022.37.e214.

[13] E. Jaleniauskiene and J. Kasperiuniene, "Infographics in higher education: A scoping review," E-Learning and Digital Media, vol. 20, no. 2, pp. 191–206, Mar. 2023, doi: 10.1177/20427530221107774.

[14] O. Fragou and M. Papadopoulou, "Exploring infographic design in higher education context: towards a modular evaluation framework," Journal of Visual Literacy, vol. 39, no. 1, pp. 1–22, Jan. 2020, doi: 10.1080/1051144X.2020.1737904.

[15] Kaddoura, M. A. (2011), "Critical Thinking Skills of Nursing Students in Lecture-Based Teaching and Case-Based Learning," International Journal for the Scholarship of Teaching and Learning, 5(2). doi: 10.20429/ijsotl.2011.050220.

[16] Rea Lavi et. al. The Evolution of an Interdisciplinary case-Based Learning First-Year Course. American Society for Engineering Education, 2023. doi: 10.18260/1-2–4451

[17] T. Keane, T. Linden, P. Hernandez-Martinez, A. Molnar, and A. Blicblau, "Digital technologies: students' expectations and experiences during their transition from high school to university," Educ Inf Technol (Dordr), vol. 28, no. 1, pp. 857–877, Jan. 2023, doi: 10.1007/s10639-022-11184-4.

[18] F. Ozdamli and H. Ozdal, "Developing an instructional design for the design of infographics and the evaluation of infographic usage in teaching based on teacher and student opinions," Eurasia Journal of Mathematics, Science and Technology Education, vol. 14, no. 4, pp. 1197–1219, 2018, doi: 10.29333/ejmste/81868.

[19] Dr. N. S. Alrwele, "Effects of Infographics on Student Achievement and Students' Perceptions of the Impacts of Infographics," Journal of Education and Human Development, vol. 6, no. 3, 2017, doi: 10.15640/jehd.v6n3a12.

[20] Ş. Elaldı and T. Çifçi, "The effectiveness of using infographics on academic achievement: A meta-analysis and a meta-thematic analysis," Journal of Pedagogical Research, vol. 5, no. 4, pp. 92–118, Dec. 2021, doi: 10.33902/JPR.2021473498.

[21] Al-Mohammadi, N. (2017). Effectiveness of using infographics as an approach for teaching programming fundamentals on developing analytical thinking skills for high school students in the city of Makkah in Saudi Arabia. Global Journal of Educational Studies, 3(1), 22-42. https://doi.org/10.5296/gjes.v3i1.10854.

[22] J. Prümmer, T. van Steen, and B. van den Berg, "A systematic review of current cybersecurity training methods," Comput. Secur., vol. 136, no. C, Jan. 2024, doi: 10.1016/j.cose.2023.103585.