

Safeguarding Digital Classrooms: Cybersecurity Implications of AI-Driven Tools in Cambodian Education

Sovannaroeth Chheang^{1*}, Sovanna Huot²

1.*Corresponding author: Sovanna Elton Foreign Language School (SELS), Cambodia, ORCID: <https://orcid.org/0009-0007-3382-7169>, sovannaroeth.chheang99@gmail.com

2. National Institute of Education (NIE), Phnom Penh, Cambodia
ORCID: <https://orcid.org/0009-0006-8335-442X>, shuot@polscience.du.ac.in

To cite this article: Chheang, S., & Huot, S. (2026). Safeguarding Digital Classrooms: Cybersecurity Implications of AI-Driven Tools in Cambodian Education. *Journal of Education Innovation and Language Teaching (JEILT)*, 2 (1), 24-46

Abstract

In Cambodia, both universities and schools are using new artificial intelligence tools, such as Learning Management Systems (LMS) and automated proctoring systems. With these tools, however, important questions about cybersecurity remain unanswered. This article examines cybersecurity concerns associated with Cambodia's increasing use of foreign providers and cross-border platforms of AI in education. The author analyses primary research results based on local case studies from Phnom Penh and Siem Reap and provides a comparative analysis of other countries in the ASEAN region. The author sheds light on some of the most important educational, structural, and policy-related weaknesses of the education system in Cambodia. Some of the most important weaknesses documented in the research include the lack of effective data governance, reliance on proprietary, high-risk technologies, the absence of a formal incident response, the lack of digital skills among educators and students, and the lack of effective data governance. The absence of the Personal Data Protection Law and the Cybercrime Law only make these policy gaps worse and increases the risks to data sovereignty and the rights of students. The author provides a set of recommendations that are the result of a collaboration among educators, policymakers, tech providers, civil society, and AI developers. The recommendations include the establishment of digital trust, improved privacy regulations, the localization of educational AI, the incorporation of digital literacy into the curriculum, and the establishment of new public procurement regulations that will enhance the cybersecurity of educational institutions.

Keywords: *Cybersecurity in Education, AI in Cambodian Schools, Data Protection and Privacy, Educational Sovereignty, AI and Surveillance, Digital Ethics*

I. Introduction

The Cambodian education sector experienced rapid digitalization as an effect of the COVID pandemic. In response to school closures, the Ministry of Education, Youth and Sport (MoEYS) shifted to digital formats to ensure learning continued. Education staff began using digital Learning Management Systems (LMS), such as Moodle and Google Classroom and communicating with students on the social media platforms Telegram and Facebook Messenger (MoEYS, 2022; UNESCO, 2021). While initially the use of these tools was meant to be temporary, they became part of Cambodia's educational ecosystem and established a basis for more lasting integration of digital and potential artificial intelligence (AI) technologies. Holmes et al. (2019) describe AI in education as a potential positive force that can help automate administrative work, customize learning experiences, and improve access to education. In Cambodia, these tools include AI software that assists with grading, tutoring apps like Khanmigo and ChatGPT, online proctoring tools like Exam.net, and plagiarism detection software like Turnitin and Grammarly. These technologies are not widely used yet, but are beginning to be used more frequently, especially in urban-based universities and among providers of private education (ITU, 2022). AI-based tools are used more often without formal integration, with teachers and students using unsecured, unregulated controls, and unsupervised trial tools (UNESCO, 2021).

On the other hand, the rapid use of new tools has outpaced implementation of proper cybersecurity and digital literacy education. Only increasing cyber-attacks and education sector are now being attacked from all the problems of phishing, ransomware, data breaches, and surveillance. It is a concern in Cambodia also, where schools often use old hardware, shared login accounts, and other unsecure systems with poor data governance (CCHR, 2021). The concern stems from the factors which stress the reliance on foreign-based AI tools, especially those using external cloud services²¹. As noted by Cavoukian (2009), the use of foreign cloud services raises issues of data sovereignty and user sovereignty, especially in the case of the entities in control of cloud service. While data control, including facial recognition data and behavioural data, as well as psychological and academic data

involves the users themselves, such services clouding foreign data control on the users from Cambodia. Such services, in cloud control, disperse data, and while using on the students, the data is yielded.

In Cambodia, tools are frequently adopted, including AI, before terms of service, and data policies, and algorithms are assessed (Huot & Loch, 2025a; Young, 2021). Students therefore are data privacy, data bias and behavioural surveillance of AI systems use). Limiting use (paying or free) impacts exposure (CCHR, 2022; Holmes et al., 2019). In Cambodia, Binns et al. (2018) stress the importance of both law & regulation; in this case, legal accountability and oversight (the third missing mechanism). In contrast, the Cambodian Centre for Human Rights (CCHR) assesses reliance on foreign AI tools and cloud services without the use of algorithms and the availability of data services in Cambodian legal and regulatory systems as the imposition of conditions with severe limitations on the data service (risk). In the absence of data policies, cloud service data control is exercised, while the reliance on software is provided (CCHR, 2022; Holmes et al., 2019). While AI tools are provided free of charge, the students become the subjects of behavioural monitoring and surveillance practices.

The intention of this study is to acknowledge the risks and focus on embedding frameworks of cybersecurity and ethics that need to accompany positive changes resulting from the use of AI in education, such as improving learning outcomes and decreasing teachers' workloads. As such, this study has the following objectives:

1. To analyze potential risks to cybersecurity associated with the use of AI in Cambodian classrooms.
2. To contextualize safeguarding and cybersecurity of digital classroom with AI.
3. To outline evidence-based reform, being implemented in collaboration with a diverse set of cybersecurity frameworks and AI in education.

II. Conceptual Framework

AI Utilization in Education Sector

Automated intelligent systems in education encompass the many facets of human thought, with understanding and critical thinking. These systems perform automated interactions in the teaching, learning, and evaluation

processes. The scholarly community recognizes the application of AI in education as an ecosystem of sub-education applications that integrate machine learning, natural language processing, and data analysis, which in turn reconfigure the distribution of educational authority, learner psychosocial and academic support, and assessment systems (Luckin & Holmes, 2016). While the oldest educational styles focused on the digitization of information, the AI educational systems alter the processes of learning analytics, education, and evaluation through continuous data capture and algorithm-based predictions (Holmes et al., 2019). With the sociological and political perspective, the role of AI-based education systems in setting the parameters of educational governance is significant. It shows an increasing influence of educational systems in establishing and reinforcing a private set of regulations that govern educational control, the learning process, and the responsibilities of educational institutions.

Educational AI-tools can be categorized into three types, as such automated assessment tools and writing support tools, intelligent tutoring systems and chatbots, and AI surveillance and proctoring tools (Huot, 2025; Luckin & Holmes, 2016). Writing support tools and automated assessment tools (such as plagiarism detection, grammar feedback systems, and automated scoring tools) assist in the evaluation of writing and scoring assessments. These tools are designed to be efficient and uniform in their assessments, but they undercut valuable aspects of the evaluation process by evaluating writing using proprietary systems and setting evaluation metrics that are not disclosed to the writer (Holmes et al., 2019). Some of the intelligent tutoring systems (ITS) and chatbots enable students to engage with the system in a manner similar to that of a tutor. Students can ask questions and request explanations, and the system will provide guidance. This can be done at times that are not during formal classes (VanLehn, 2011). The final category, AI surveillance and proctoring tools, use surveillance tools (webcams, keystroke tracking, eye tracking, etc.) to monitor students' behaviour and biometrics to assess their risk and behaviour (Williamson, 2019). All these tools share similar educational goals. The aim of the system is to provide educational support using data, feedback loops, and computer processing (Holmes et al., 2019; Huot & Loch, 2025c).

Systems of educational governance recognize the pedagogical importance of AI/ML based technologies, but more importantly, the systems identify the governance structures of decision rights in education, which accesses to what data, regulates scope of data usage, keeps the data user accountable, outlines the applicable standards of data user misconduct, and limits the user's rights in the event that, an error, bias, or data breach occurs. The scholars of algorithmic accountability warn that educational AI could eventually lead to a regime of educational oppression in which institutions rely upon outputs that they cannot fully assess, while users are subjected to decisions that they cannot meaningfully challenge (Veale & Binns, 2017). In such cases, the educational benefits of personalization and efficiency that such systems will provide must be counterbalanced with the political risks that accompany opaque governance, unregulated data flows, and an unequal ability to govern data systems.

Adoption of Technologies in Cambodian Classrooms

In Cambodia, the adaptation of AI educational tools can be constructed as asymmetric and hybrid. The use of these tools develops quickly, focusing on the connectivity, English language skills, and institutional resources, while the educational tools remain underdeveloped in other areas. Cambodia's national digital transformation agenda explicitly states digitalization as a pathway for development with long-term effects, as seen in the Cambodia Digital Economy and Society Policy Framework 2021-2035 and Cambodia Digital Government Policy 2022-2035 (RGC, 2021, 2022). In these policies, digital systems and digitalization are centered as tools for modernization, improving public service, and developing the country's human resources. Such policies create an opportunity for the digitalization of the education sector, with increased use of platforms, digital partnerships and services, which often use AI tools.

Within institutions, the adoption of AI tends to transpire through three pathways. First, some universities and higher-resourced secondary schools, especially in locales with prevalent English-medium instruction, incorporate automated writing and plagiarism detection systems into their academic writing and assessment processes. Second, in the absence of formal policy frameworks, the teachers and students use the generative AI and tutoring

applications in an informal fashion to summarize lessons, translate Khmer and English, draft outlines, and practice target language skills. Third, in the remote or blended learning contexts, schools use the monitoring tools integrated into the learning management systems or online assessment platforms that, even when introduced as integrity features, may promote surveillance (Williamson, 2019). Cambodia's current landscape shows one dominant feature: reliance on foreign-developed platforms. Given that such platforms' terms of service, data hosting, and model training practices are clouded by foreign jurisdictions. Cambodia lacks data oversight and audit powers. At the same time, Cambodia's legal drafts environment concerning the protection of personal data has been evolving, but not in a consolidated fully built legal regime.

Reporting in 2025 mentions that Cambodia published a draft law on the protection of personal data and that the law has been commented on, suggesting that law is expected to be implemented, but not fully operational. This effectively means that, for Cambodian institutions, the governance of AI tools is more a function of institutional capacity (contracts, procurement, IT, academic integrity) than of applicable national data protection systems and frameworks that are enforceable. These conditions result in a distinct pattern: Cambodian education is not AI-free. AI is present in education in socially uneven ways, determined by access to language, devices, digital literacy of teachers, and the capacity of institutions to convert broad digital policy ambitions into the specific governance frameworks in classrooms. The Education Strategic Plan 2024-2028 emphasizes that digital transformation and frameworks of the national policy are integral guiding documents for education policy, reiterating a preferred trajectory, even when the pace of implementation is uneven (MoEYS, 2024).

Works of AI Tools in Data Flows and Processing Mechanisms

With ethical and cybersecurity perspective, understanding the data lifecycle is essential when assessing AI in education. Most AI-powered tools function on the same four-cycle process, such as input and capture, transmission and processing, feedback and action, retention and secondary use. The users create some type of content, for example, an essay, a query to a bot, an audio response, or a log into an online assessment. This input, along with

metadata, is captured and is, in some cases, tied to timestamps, device IDs, and interaction logs that can provide clues about a user's learning behavior and patterns (Holmes et al., 2019). In the second stage, data is sent to remote (cloud-based) servers where proprietary algorithms perform various tasks such as natural language parsing, similarity checks, scoring, or conversation generation. In the third stage, data structures (e.g., feedback, scores, flags, suggestions) determine the revision behaviors of the students, the score assessment of the teachers, or the decision of the institution. In the end, data are retained for a certain period, and based on their operating policies and user agreements, they can be reused to improve services, train algorithms, or update new and improved filtering systems.

Scholars argue that this data is not politically neutral. When educational platforms translate learning into behavioral traces and predictive patterns, students and teachers usually cannot access the same granule levels of inferences that platforms and vendors can generate, creating marked asymmetries of visibility and power (Pangrazio et al., 2023; Raffaghelli et al., 2020). These digital traces may include highly sensitive, student-referenced materials, such as writings, mistakes, topics, and histories of interactions. It is also sensitive when things are retained or reused. Furthermore, digital records may also be sensitive in cross-border jurisdictional circumstances when parent companies and servers are located outside the user's country (Hok et al., 2026; Huot & Hok, 2025). Legally, the user's country will have limited access to breaches and disputes of the records. In Cambodia, where national frameworks are legally in a consolidation phase, the importance of good record keeping and institutional procurement is magnified by these frameworks, as are the practices of consent and disclosure (Huot & Loch, 2025c).

The processing stage also runs the risk of systematic error and bias. It is particularly the case when Technology Integrated Language Learning (TILL) tools are biased based on a lack of diversity in the training data used by the tools (Lee et al., 2025). The evaluative criteria for the tools tend to focus on the hegemonic center, which overlooks the outer circles of English (approximately, Asian countries) and penalizes peripheral outer, resulting in reinforcing and reproducing stark cultural blindness (Kachru, 1985). The

problem is exacerbated when there is limited data in the Khmer language. This aligns with large-scale language technology critiques that highlight bias, a lack of representation, and the tendency to construct incorrect answers that present to users with unjustified certainty (Bender et al., 2021). If students are misled by these answers and lack the necessary skills to verify them, AI can quietly change the way students learn.

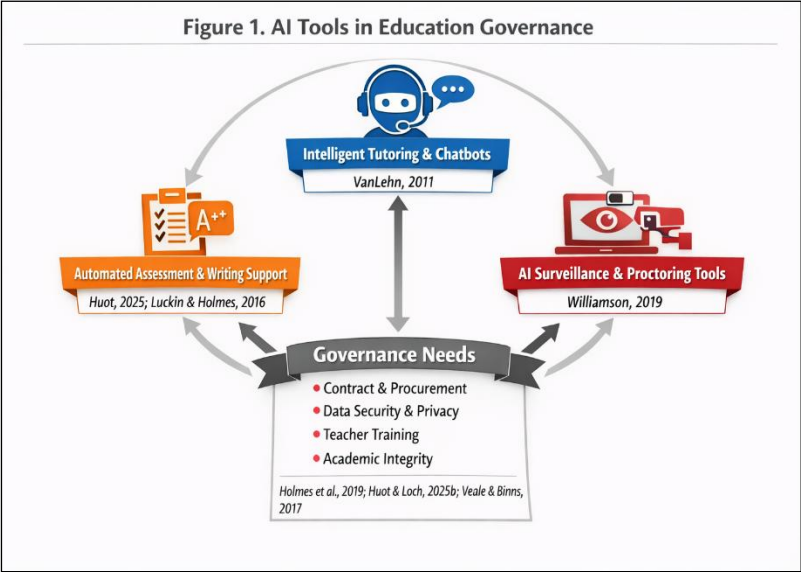
The Concerns of Student Privacy and Cybersecurity

When educational institutions use AI-based technologies, they increase the chances of suffering a cyberattack, given AI tools create new access points and data collection services (Huot & Loch, 2025b). The focal point of a school's or a university's cyber risk is not the sensationalist notion of being hacked, but rather the mundane gaps like unprotected passwords, shared logins, unprotected networks, and the general lack of access control and incident response plans (Huot & Such, 2025). When slavery, social security, and (in the case of automated proctoring) behavioral or emotional surveillance data are collected, these gaps take on a greater level of risk. Two issues, in particular, are troubling from a governance and privacy perspective. First, there is the normalization of surveillance. PAI (proctoring artificial intelligence) systems may not simply facilitate assessments but may chill student behaviors and foster a lack of trust through the transformation of assessments into constant surveillance, especially when consent is weak and alternatives are not offered (Williamson, 2019). The second is the lack of accountability. Students may find themselves in positions of consequence with little or no recourse when automated systems flag them for suspicious behaviors or originality detection (Huot & Tep, 2025).

This situation directly contradicts accountability and contestability principles of governance (Veale & Binns, 2017). The lack of control and opaque decision made also speaks to the absence of justice. This is one of the reasons why privacy scholars suggest that the adoption of privacy by design approaches (data minimization, purpose specification, and appropriate security) be made standard, as opposed to optional (Cavoukian, 2009).

In Cambodia, these implications are interwoven with the country's digital transformation objectives. As the digital policy frameworks aim to leapfrog

digital adoption, there is a need to ensure that in the education sector, pace of scaling is matched with adequacy of governance (Huot & Loch, 2025b). Given that Cambodia is on record as moving toward comprehensive data protection via draft law, as opposed to a historically defunct enforcement regime, the burden on institutions is greater; contracts, procurement policies, teacher training, and student guidance must fulfil most of the governance needs, as shown in Figure 1.



III. AI Frameworks and Cybersecurity in Cambodian Education

In terms of legality and institutions, the governance of AI in education in Cambodia is emergent and uneven. Recent national dialogues include digital transformation as an aspect of modernisation, but the required regulatory frameworks for the governance of AI, educational data, and cybersecurity remain incomplete (Huot & Em, 2025a). Cambodia’s digital readiness reports by UNESCO highlight advancements in parts of the country’s digital policy, but there is still a lack of core elements of the ethical and rights-based AI frameworks, especially those concerning data protection, responsibility, and the operationalisation of frameworks concerning the same (UNESCO,

2023, 2024). This is particularly true for education as students are likely to be the most affected as the use of AI tools in education is becoming commonplace, and such tools collect personal data, sensitive behavioural and learning data, as well as data related to the users' interactions.

Cambodia's draft law on personal data protection is an important legal development in this area. The Ministry of Posts and Telecommunications (2021) has published multiple drafts, seeking to capture the essence of other laws in terms of the principles of lawful processing, the protection of personal data and its processing, data subject's rights, purpose limitation, data protection and security, and data transfer controls (Ministry of Posts and Telecommunications, 2021). While this may indicate progress on Cambodia's legal protection of personal data to meet global requirements, the problem is Cambodia's legal protection of personal data is not lacking in legal terminology. It is lacking in the operationalization of the formal legal structures in different sectors. UNESCO (2024) noted that Cambodia has yet to develop a sufficient governance framework that turns generalized digital principles into enforceable, operational frameworks in specific sectors. This is particularly true in education. The draft law does not specify how data related to minors, online proctoring, biometric data, and learning analytics should be dealt with.

The Cambodia's draft law on personal data protection, International Center for Not-for-Profit Law (2025) also argues that the draft framework is too vague and is not attentive enough to risks pertaining to specific sectors. As a result, schools and universities have no actionable ways to address how to handle student data connected to AI systems that are located overseas, what multinational companies operate educational platforms, or how to handle student data contained in cloud systems outside of Cambodia (Huot et al., 2024). While the draft law mentions informed consent, sensitive data, and cross-border data flows, these remain under-specified concerning educational governance. Cambodia still lacks a developed supervisory framework for schools to address questions of data retention, obtainment of parental consent, and institutional accountability regarding the unlawful or excessive collection of student data (Lee et al., 2025). In this sense, the

law lacks the guidance needed to effectively address these issues concerning the education system and governance of AI-driven educational systems.

A related trend has emerged in cyberspace. Drafted several years ago, Cambodia's cybercrime law has generated considerable public comment, but most of the feedback seems to address crime, surveillance, interruptions, and state security, rather than the everyday protections of an institutional nature. The scope of the draft law has the potential of negatively impacting civil liberties, while providing little, if any, protective legal coverage for the average user (Human Rights Watch, 2020). From an educational point of view, the greatest shortcomings of the cybercrime draft law are that such legislation will not address the everyday governance issues that AI will create in classrooms, nor impose any obligations on schools for breach notifications, protect children on educational platforms, impose standards for surveillance in the AI assessment, or establish the minimum cyber protections for the digital teaching resources (Huot & Em, 2025b). For this reason, the draft cybercrime law will most certainly not address the educational cyber protections that Cambodian institutions so urgently need. While the MoEYS (2024) is implementing digital reforms on an organizational level, it is yet to formulate an all-encompassing AI governance framework applicable to schools and universities, outlining the integration of ICT, the modernization of processes, and the incorporation of online learning into the system; however, it is silent on the ethics of AI, the governance of educational data, accountable cybersecurity, and the regulation of EdTech procurement. UNESCO (2024) also reports that gaps remain for Cambodia in the preparation of institutions and the governance of coordination. Therefore, the adoption of AI in education is fragmented, internally improvised, or vendor driven in the absence of national directives. Teachers, students, administrators, and parents remain without adequate support on what is safe, legal, and ethically considered to be the appropriate use of AI in education (MoEYS, 2021).

Comparisons with other countries show Cambodia's current state is not bound to happen. A country that shows this is Singapore, as it has already incorporated a working data protection regime. The Personal Data Protection Act (PDPA) provides the duties of the Data Protection Officer and

has issued Advisory Guidelines for the Education Sector which speak to issues of consent, student records, biometrics, and breaches (Personal Data Protection Commission Singapore, 2019, 2024). In this case, educational digital innovation is integrated to a solid legal framework. Vietnam illustrates this as well in a different way. The more state-centred control in its cybersecurity and its personal data protection regulations, i.e., Decree No. 13/2023/ND-CP, show more in its recognition of the need for a more enforceable governance to digital education than institutional improvisation (Government of Vietnam, 2023; U.S. International Trade Administration, 2022). In comparison to these countries, Cambodia shows a more primitive out the phases of institutionalization.

The issues with the law are also aggravated by the limitations of the educational institutions themselves. In Cambodia, UNESCO (2024) emphasizes the importance of having more effective human and institutional capacities. Moreover, the guidelines to the Cambodian Child Online Protection document recognize the growing dangers of digital technology and the institutions and the industry's responsibility to combat it (Ministry of Posts and Telecommunications, 2021). In most of Cambodian educational institutions, the relying on cheap, mainstream foreign platforms used to be more common; now, it is used in most of them. There are serious dangers related to unauthorized access and data loss, and weak accountability. These include the use of personal devices, informal cloud data storage, and data storage on institutional system. Many teachers are left without adequate training in the use of cyber-hygiene, the ethics of AI, and the privacy restrictions. On the other hand, Huot and Tep (2025) suggest that students may engage with AI casually and without sufficient awareness of the legal and ethical implications of the digital footprints they create.

At an organizational level, the lack of formal procedures heightens these risks. Cyber incidents become difficult to capture, manage and address when schools do not have procedures for breach reporting, incident escalation, digital forensics, vendor review, and learning after incidents. Cambodia's ability to implement Trustworthy AI in education hinges on panopticons (UNESCO, 2024). Educational institutions, in the absence of

these structures, must improvise, and improvisation leads to poor and inconsistent protection, weak remedy, and loss of trust.

Cambodia has the digital ambition to implement an education system that uses artificial intelligence and is far more advanced than the ability to protect the system. In relation to this, Zuboff's (2023) critique of the asymmetry of data relationships is pertinent. She argues that in the digital system, the knowledge, the ability to survey, and the power to make decisions are concentrated in the hands of the owners of the platforms, while those who create the data are dependent and exposed. In the Cambodian educational system, this is evidenced in the heavy dependence on foreign platforms, the lack of oversight of the education sector, and the restricted ability of educational institutions to control the data of the students (Huot & Such, 2025). Thus, the use of AI and Cybersecurity in Education in Cambodia is much more than a technical issue, it is a matter of law, policy, and institutional frameworks that require the collaboration of policymakers, ministries, regulators, school administrators, and teachers.

IV. Emerging Trends of Educational AI-Tools and Cybersecurity

When designing meaningful and realistic protections, discussions of AI ethics and cybersecurity should focus on concrete rather than abstract policy engagements. In Cambodia, several digital educational risks have been informally handled, reactively or with limited institutional considerations. However, recent cases from Cambodia and other countries show that the adoption of AI tools is faster than the ethical, cyber, and institutional response frameworks (Huot & Loch, 2025b). Digital education scholars warn that in schools; technological innovations are never neutral or purely technical. They are influenced by governance, organizational culture, and the capacity of educational systems to ensure learners' protective rights in practice (UNESCO, 2024; Williamson, 2017, 2019).

A growing trend has resulted in increased vulnerability in educational institutions to phishing, credential harvesting, and other basic but effective cyberattacks. Some educational institutions, particularly schools and universities, exhibit digital systems that are reliant upon traditional approaches (weak accounts, uninformed users, and an underdeveloped incident-response framework) (Huot & Loch, 2025d). Cybersecurity experts

express great concern that inadequate digital literacy, weak password use, and poor social engineering awareness continue to be among the greatest vulnerabilities in educational institutions (ITU, 2022; OECD, 2021). In Cambodia, these vulnerabilities are exacerbated by the inconsistent capacity of institutions and a lack of unambiguous breach-response communication protocols (Huot & Loch, 2025c). In the absence of clear communication protocols, institutions that fail to engage in multi-factor authentication, employee cyber hygiene training, and the establishment of cyber incident rapid reporting systems broaden the range of negative impacts beyond cyber disruptions to transgress privacy, distort educational integrity, and erode trust in the institution.

A second leading trend is the rapid emergence of AI-based monitoring and assessment tools, particularly online proctoring systems. While these tools are marketed as addressing concerns of fairness, efficiency, and academic dishonesty, researchers argue that they heighten the surveillance, stress, and data harvesting within educational settings. Williamson (2019) believes that educational technology is increasingly driven by what she calls techno-solutionism, where complex educational and moral dilemmas are reframed within the context of automated surveillance and control. In the same vein, UNESCO (2024) draws attention to the fact that, in the absence of appropriate privacy, transparency, and human oversight, the adoption of AI in education may create additional risks, and perhaps even more so for schools. Continuous monitoring through facial recognition, screen capture, keystroke tracking, and behavioural flagging systems can turn educational assessments into surveillance rather than equitable assessment.

This issue is even more concerning when parents and students lack any plausible means of comprehending the system. Informed consent is not a mere formality. Users must have the opportunity to understand the scope of data collection, duration of data retention, location of data processing, and the identity of data users. Privacy and digital governance experts argue that biometric and behavioural data are particularly sensitive and warrant additional protection, as such data are highly personal, difficult to revoke, and prone to misuse when processed and transferred (Raffaghelli et al., 2020; UNESCO, 2024). Without examining foreign vendor privacy policies

and contracts before implementing foreign-funded AI systems, schools impose extreme surveillance on students and, even worse, students are not aware of what surveillance is being conducted.

A growing trend last seen at educational institutions is the reliance on outside vendors - the systems of which are rarely evaluated independently. Third-party AI tools are introduced under the guise of increased efficiency, innovation, or security (Huot et al., 2024). In fact, the internal workings, error rates, and biases of these systems are often unknown to the educational institutions. Scholars of AI governance warn that accountability gaps may arise from such absence of transparency. For example, automated systems may tentatively penalize users for non-misconduct, including unreliable internet connection, poor lighting, or distracting disabilities. Automated systems may misclassify or generate false positives (UNESCO, 2024; Williamson et al., 2020). The consequences of these systems in educational environments extend beyond mere technical errors. These systems can contribute to the shaping and redefining of trust, dignity, and the overall assessment and disciplinary processes of students.

What regional examples have shown teaching AI for example. Sometimes educational AI is perceived as vendor lock-in, low accountability, surveillance, etc., even in advanced digital environments (Huot & Em, 2025a). Therefore, what is relevant is not if technology is integrated, but how it is governed, justified, and contextualized. Digital governance literature suggests that effective protection is the result of multiple, layered approaches to governance. Transparent and secured procurement, independent vendor reviews, data minimization, breach notification, appeals, and regular oversight in the name of ethics all represent the kind of layered approaches that the literature recommends (OECD, 2021; UNESCO, 2024). In the absence of such, educational AI is likely to deepen the institutional vulnerability it is designed to mitigate.

A number of lessons can be drawn from the developments of this case. First, AI systems are not neutral. Scholars contend that automated systems tend to mirror the values, biases, and priorities that are baked into the system's design, dataset, and institutional use (Williamson, 2017; Zuboff, 2023). When deployed without an ethical framework, such tools may legitimize

surveillance, hide the dynamics of power, and limit the capacity of students to challenge the decisions of an automated system. Second, knowledge and regional learning are important. At the level of the ASEAN, Cambodia can engage in dialogues, collaborative studies, and the cross-border exchange of policies concerning the ethics of AI, cybersecurity, and safe digital education (UNESCO, 2017). Nonetheless, learning by comparison should not equal an uncritical adoption of policies. Effective governance will have to be context-specific to Cambodia's legal framework, digital and governance infrastructure, administrative capacity, and educational philosophy. Finally, digital education should not be evaluated on the availability of instruments alone. Access is important, but it is not enough. As Selwyn (2021) remarked, educational technology should be critiqued in relation to pedagogy, rights, and power, and not in a framework of mere instrumentalism and efficiency. Cambodia is at a critical juncture. The country can choose a path of continued adoption of unregulated and fragmented AI tools, which allows institutions to improvise after damage has been done. Alternatively, it can take a considered approach where AI and digital transformation are used alongside strong ethical, safe, transparent, and educational practices. For Cambodia to achieve sustainability in the use of AI in education, it will require further innovation and infrastructure. More importantly, it will require placing the rights of the learners, accountability of the institutions, and the trust of the public at the core of the digital governance model.

V. CONCLUSIONS

This recent study focused on the application of AI and data-driven digital technologies in the educational sector. Cambodia took steps towards the digitalization of education. However, the institutional framework would serve to protect the educational stakeholders from the risks posed by the inadequate protection of data, oversight, transparency of the algorithms, academic fraud, fragile digital framework, and an overreliance on external governance of digital tools. Cambodian education system lacked autonomy and self-reliance to develop sophisticated and effective digital education delivery systems and digital service systems to manage and support education. Cambodia's reliance on foreign systems places their education digital delivery systems at risk of dependence on unregulated educational

services and provider systems that captured the education system's data. Therefore, education system should use other digital services, and effective digital-services could be integrated to ensure the education systems. In this context, initiatives needed to be viewed as technological defences and ethical governance of technology in a transparent and responsible manner. Without ability to audit platforms, set boundaries, or build local solutions, Cambodia was likely to become an educational future consumer instead of an educational future producer. The focus should be placed on ensuring equity, safety, dignity, trust, and people centric development.

Reference

- Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? In L. Irani, S. Kannan, M. Mitchell, & D. Robinson (Eds.), *Proceedings of the 2021 ACM conference on fairness, accountability, and transparency* (pp. 610–623). Association for Computing Machinery, New York, NY, United States. <https://doi.org/10.1145/3442188.3445922>
- Binns, R., Van Kleek, M., Veale, M., Lyngs, U., Zhao, J., & Shadbolt, N. (2018). 'It's reducing a human being to a percentage' perceptions of justice in algorithmic decisions. In R. Mandryk, M. Hancock, M. Perry, & A. Cox (Eds.), *Proceedings of the 2018 Chi conference on human factors in computing systems* (pp. 1–14). <https://doi.org/10.1145/3173574.3173951>
- Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, 5, 1–5. https://student.cs.uwaterloo.ca/~cs492/papers/7foundationprinciples_longer.pdf
- CCHR. (2021). *Legal analysis of the draft law on cybersecurity in Cambodia*. Cambodian Center for Human Rights. <https://cchrcambodia.org>
- CCHR. (2022). *The state of freedom of expression, press freedom, and access to information in Cambodia*. Cambodian Center for Human Rights. <https://media.business-humanrights.org/>

[media/documents/CCHR_Report_on_State_of_Freedom_of_Expression_and_Access_to_Information_FINAL__mxbgkOy.pdf](#)

- Government of Vietnam. (2023). *Decree No. 13/2023/ND-CP on personal data protection*. Government of Vietnam. <https://vanban.chinhphu.vn/?docid=207352&pageid=27160>
- Hok, C., Phin, K., Saroth, C., Sakhorn, S., Chheang, S., & Huot, S. (2026). Advancing ELT in Cambodia: Sustainability, digital inclusion, and culturally responsive pedagogy. *The Rubrics*, 8(8), 79–99. <https://doi.org/10.5281/zenodo.18149324>
- Holmes, W., Bialik, M., & Fadel, C. (2019). *Artificial intelligence in education promises and implications for teaching and learning*. Center for Curriculum Redesign.
- Human Rights Watch. (2020). *Cambodia: Scrap draft cybercrime law – Law would expand surveillance, threats to free expression online*. Human Rights Watch,. <https://www.hrw.org/news/2020/11/13/cambodia-scrap-draft-cybercrime-law>
- Huot, S. (2025). Digital tutors in the kingdom: Exploring ChatGPT’s influence on Cambodian students’ academic and cognitive growth. In J. D. Pandya & K. C. Patel (Eds.), *Interdisciplinary insights: Exploring multiple perspectives* (Vol. 2, pp. 36–54). Meadow Publication.
- Huot, S., & Em, S. (2025a). Effective strategies of English teaching in Cambodia’s underserved communities: Bridging digital divide to access education quality. *Journal of Education Innovation and Language Teaching (JEILT)*, 1(1), 53–77. <https://doi.org/10.63381/jeilt.v1i1.38>
- Huot, S., & Em, S. (2025b). Integrating English language teaching with environmental sustainability: A comprehensive review of pedagogical strategies and global impacts. *Cambodian Journal of Educational and Social Sciences (CJESS)*, 1(2), 83–95. <https://doi.org/10.69496/cjess.v2i2.68>
- Huot, S., & Hok, C. (2025). Enhancing English language teaching for multilingual learners: Leveraging heritage languages in the

- classroom. *Journal of Social and Educational Research*, 4(1), 87–95. <https://doi.org/10.5281/zenodo.15698964>
- Huot, S., & Loch, S. (2025a). Buddhist and yogic dialogues on inner ecology: Comparative insights for education and governance in the global South. *International Council for Education Research and Training*, 4(4), 264–285. <https://doi.org/10.59231/SARI7879>
- Huot, S., & Loch, S. (2025b). Digital practices in Cambodian EFL classrooms: Teacher narratives from remote learning. In K. Khette & Tayade (Eds.), *Proceeding of one day national conference on English language, literature, cultural studies and media studies* (Vol. 2, pp. 19–31). Centre for Learning, Research and Development, Savda, Maharashtra. <https://doi.org/10.5281/zenodo.16921807>
- Huot, S., & Loch, S. (2025c). Educating in the age of AI: Preparing Cambodian teachers and students for an AI-augmented learning future. *Journal of Educational Technology and E-Learning Innovations*, 1(2), 31–38. <https://doi.org/10.54536/jeteli.v1i2.5170>
- Huot, S., & Loch, S. (2025d). From rote to reflective: Integrating ChatGPT to transform learning outcomes in Cambodian education. *International Journal of Language and Literary Studies*, 7(4), 1–15. <https://doi.org/10.36892/ijlls.v7i4.2188>
- Huot, S., Sam, R., & Nguon, T. (2024). Influencing factors in teaching career choices in Cambodia in teacher education colleges: A conceptual framework. *European Journal of Arts, Humanities and Social Sciences*, 1(6), 97–108. [https://doi.org/10.59324/ejahss.2024.1\(6\).11](https://doi.org/10.59324/ejahss.2024.1(6).11)
- Huot, S., & Such, C. (2025). Leveraging social media for language learning: Opportunities and challenges. *Journal of Education Innovation and Language Teaching (JEILT)*, 1(2), 10–29. <https://doi.org/10.63381/jeilt.v1i2.56>
- Huot, S., & Tep, P. (2025). Advancing ChatGPT for pedagogical innovation in Cambodia: Insight from global evidence and

- local implications. *The Context: Journal of English Studies*, 12(4), 115–135. <https://doi.org/10.5281/zenodo.15806972>
- International Center for Not-for-Profit Law. (2025). *Summary analysis: Cambodia's draft law on personal data protection*. International Center for Not-for-Profit Law. https://data.opendevdevelopmentcambodia.net/en/dataset/087a5b1e-bc04-4da1-8870-c375b87e01f2/resource/fd8b0cb3-afc4-44d0-a9c8-1e482a9f7e2c/download/icnl-comments-on-cambodia-draft-law-on-personal-data-protection_july2025.pdf
- ITU. (2022). *Measuring digital development: Facts and figures 2022*. International Telecommunication Union. https://www.itu.int/dms_pub/itu-d/opb/ind/d-ind-ict_mdd-2022-pdf-e.pdf
- Kachru, B. B. (1985). Standards, codification and sociolinguistic realism: The English language in the outer circle. In R. Quirk & H. G. Widdowson (Eds.), *English in the world: Teaching and learning the language and literatures/Cambridge UP* (pp. 11–30). Cambridge University Press.
- Lee, S., Jeon, J., McKinley, J., & Rose, H. (2025). Generative AI and English language teaching: A global Englishes perspective. *Annual Review of Applied Linguistics*, 45, 85–108. <https://doi.org/10.1017/S0267190525100184>
- Luckin, R., & Holmes, W. (2016). *Intelligence unleashed: An argument for AI in education*. Pearson. <https://www.pearson.com/content/dam/corporate/glob...>
- Ministry of Posts and Telecommunications. (2021). *Cambodia digital economy and society policy framework 2021–2035*. Royal Government of Cambodia, Retrieved from <https://asset.cambodia.gov.kh/mptc/media/EN-Policy-Framework-of-Digital-Economy-and-Society.pdf>
- MoEYS. (2021). *ICT in education roadmap 2021–2025*. Phnom Penh, Cambodia: Ministry of Education, Youth and Sport. <https://moeys.gov.kh/storage/uploads/documents/65dd5f904dc9d.pdf>

- MoEYS. (2022). *Education statistics and indicators 2021–2022*. Phnom Penh. <https://moeys.gov.kh/en/education-statistics/document-5240>
- MoEYS. (2024). *Education strategic plan 2024-2028*. Phnom Penh, Cambodia: Ministry of Education, Youth and Sport. <https://moeys.gov.kh/storage/uploads/documents//67316f9d3a57f.pdf>
- OECD. (2021). *21st-century readers: Developing literacy skills in a digital world*. Paris: Organisation for Economic Co-operation and Development Publishing. <https://doi.org/10.1787/a83d84cb-en>
- Pangrazio, L., Selwyn, N., & Cumbo, B. (2023). Tracking technology: Exploring student experiences of school datafication. *Cambridge journal of education*, 53(6), 847–862. <https://doi.org/10.1080/0305764X.2023.2215194>
- Personal Data Protection Commission Singapore. (2019). *Guide to managing data breaches 2.0*. Personal Data Protection Commission Singapore. <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/other-guides/data-breach-management/introduction-to-managing-data-breaches-2-0.pdf>
- Personal Data Protection Commission Singapore. (2024). *Advisory guidelines for the education sector*. Personal Data Protection Commission Singapore. https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-for-education-sector_25-apr-2024.pdf
- Raffaghelli, J. E., Manca, S., Stewart, B., Prinsloo, P., & Sangrà, A. (2020). Supporting the development of critical data literacies in higher education: building blocks for fair data cultures in society. *International Journal of Educational Technology in Higher Education*, 17(1), 1–22. <https://doi.org/10.1186/s41239-020-00235-w>
- RGC. (2021). *Cambodia digital government policy 2021–2035*. Royal Government of Cambodia, Phnom Penh: Ministry of Post and Telecommunications.

- https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf
- RGC. (2022). *Cambodia digital government policy 2022–2035*. Royal Government of Cambodia. https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf
- Selwyn, N. (2021). *Education and technology: Key issues and debates*. Bloomsbury Publishing.
- U.S. International Trade Administration. (2022). *Vietnam: Cybersecurity data localization requirements*. U.S. International Trade Administration. <https://www.trade.gov/market-intelligence/vietnam-cybersecurity-data-localization-requirements>
- UNESCO. (2017). *Ethical principles for safeguarding intangible cultural heritage*. UNESCO. <https://ich.unesco.org/en/ethics-and-ich-00866>
- UNESCO. (2021). *The impact of COVID-19 on early childhood education in the Asia-Pacific and Sub-Saharan Africa*. Bangkok: UNESCO. https://knowledge.unasiapacific.org/sites/default/files/2021-07/378125eng_0.pdf
- UNESCO. (2023). *Guidance for generative artificial intelligence (GenAI) in education and research: A human-centered approach*. United Nations Educational Scientific and Cultural Organization. <https://policycommons.net/artifacts/6942367/guidance-for-generative-ai-in-education-and-research/7852269>
- UNESCO. (2024). *Cambodia: Artificial intelligence readiness assessment report*. UNESCO. https://articles.unesco.org/sites/default/files/medias/fichier/s/2025/07/CAMBODIA%20-%20AI%20Readiness%20Assessment%20Report%202025_0.pdf
- VanLehn, K. (2011). The relative effectiveness of human tutoring, intelligent tutoring systems, and other tutoring systems.

- Educational psychologist*, 46(4), 197–221.
<https://doi.org/10.1080/00461520.2011.611369>
- Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. *Big Data & Society*, 4(2), 1–17.
<https://doi.org/10.1177/2053951717743530>
- Williamson, B. (2017). *Big data in education: The digital future of learning, policy and practice*. SAGE Publications Ltd.
<https://doi.org/10.4135/9781529714920>
- Williamson, B. (2019). Policy networks, performance metrics and platform markets: Charting the expanding data infrastructure of higher education. *British Journal of Educational Technology*, 50(6), 2794–2809.
<https://doi.org/10.1111/bjet.12849>
- Williamson, B., Bayne, S., & Shay, S. (2020). The datafication of teaching in Higher Education: Critical issues and perspectives. 25(4), 351–365.
<https://doi.org/10.1080/13562517.2020.1748811>
- Young, S. (2021). Internet, Facebook, competing political narratives, and political control in Cambodia. *Media Asia*, 48(1), 67–76.
<https://doi.org/10.1080/01296612.2021.1881285>
- Zuboff, S. (2023). The age of surveillance capitalism. In W. Longhofer & D. Winchester (Eds.), *Social Theory Re-Wired* (3 ed., pp. 203–213). Routledge.
<https://doi.org/10.4324/9781003320609>