EdTech Hub

Clear evidence, better decisions, more learning.

ASEAN-UK SAGE | Supporting the Advancement of Girls' Education

TOPIC BRIEF

AI in Southeast Asia: Ethical Governance of AI in Education

Assessing regional AI policy alignment and implications for learners and education systems

Date February 2026

Authors Neema Jayasinghe

DOI 10.53832/edtechhub.1179

UK International Development
Partnership | Progress | Prosperity

THE WORLD BANK

unicef for every child

@GlobalEdTechHub edtechhub.org

About this document

Recommended citation

Jayasinghe, N. (2026). *AI in Southeast Asia: Ethical Governance of AI in Education. Assessing regional AI policy alignment and implications for learners and education systems* [Topic Brief]. EdTech Hub. https://doi.org/10.53832/edtechhub.1179. Available at https://docs.edtechhub.org/lib/2VBH4GZX. Available under Creative Commons Attribution 4.0 International.

Reviewers Sangay Thinley, Jazzlyne Gunawan, and Katrina Barnes.

Acknowledgements Thanks are also due to Navindu Leelarathna and Aprillia Chrisani.

About EdTech Hub

EdTech Hub is a global research partnership. Our goal is to empower people by giving them the evidence they need to make decisions about technology in education. Our evidence library is a repository of our latest research, findings, and wider literature on EdTech. As a global partnership, we seek to make our evidence available and accessible to those who are looking for EdTech solutions worldwide.

EdTech Hub is supported by UKAid, Bill & Melinda Gates Foundation, World Bank, and UNICEF. The views in this document do not necessarily reflect the views of these organisations.

To find out more about us, go to edtechhub.org/. Our evidence library can be found at docs.edtechhub.org/lib/.

This publication has been produced by EdTech Hub as part of the ASEAN-UK Supporting the Advancement of Girls' Education (ASEAN-UK SAGE) programme. The ASEAN-UK SAGE programme is delivered by the British Council and SEAMEO Secretariat, in partnership with EdTech Hub and the Australian Council for Educational Research (ACER), and is an ASEAN cooperation programme funded by the UK. The programme aims to enhance foundational learning opportunities for all by breaking down barriers that hinder the educational achievements of girls and marginalised learners.

This material has been funded by the UK; however, the views expressed do not necessarily reflect the UK Government's official policies.

EdTech Hub's topic briefs on AI in education in Southeast Asia

Across Southeast Asia, the demand for guidance on the use of artificial intelligence (AI) has grown rapidly. EdTech Hub has engaged with a number of partners across Southeast Asia on the use of AI in education, indicating that policymakers and teachers across the region are seeking clarity on the use of AI to support teaching and learning. This reflects a need for contextualised, reliable, high-quality, and rapid research to help education stakeholders quickly understand and adapt to emerging AI in education trends and topics.

While global evidence on AI in education is expanding quickly, stakeholders across the region have highlighted the need for tools that translate this knowledge into practical, locally relevant insights. The topic briefs respond directly to this need.

The briefs examine the intersection of AI with key elements of the education ecosystem in Southeast Asia. An initial desk review of the regional AI in the education landscape surfaced several priority themes and areas of interest, leading to the development of five topic briefs in this series.

This brief examines the use of AI for marginalised learners and focuses on the question:

To what extent are private EdTech companies aligning with national and regional ethical commitments for the safe and responsible implementation of AI in education?

The other briefs in this series include:

AI in Southeast Asia: Strategic Partnerships by Delanie Honda (2026). EdTech Hub. https://doi.org/10.53832/edtechhub.1164. Available at https://docs.edtechhub.org/lib/NH9HAIW5.

AI in Southeast Asia: Marginalised learners by Iona Wotton. (2026) EdTech Hub. https://doi.org/10.53832/edtechhub.1173. Available at https://docs.edtechhub.org/lib/ZAIZ22IV.

AI in Southeast Asia: Girls' Education by Alesia Petrovets (2026). https://doi.org/10.53832/edtechhub.1180. Available at https://docs.edtechhub.org/lib/3KT6QT98.

AI in Southeast Asia: The Role of Teachers *by* Iona Wotton, Delanie Honda, & Nurhasmiza Sazalli, N. (2026) https://doi.org/10.53832/edtechhub.1178. Available at https://docs.edtechhub.org/lib/XWRW9BUJ.

Contents

Tables

Abbreviations and acronyms

AI	Artificial Intelligence
APWG	Anti-Phishing Working Group
ASEAN	Association of Southeast Asian Nations
DPA	Data Privacy Act of 2012 (Philippines)
ICO	Information Commissioner's Office (UK)
NIST	National Institute of Standards (USA)
NPC	National Privacy Commission (Philippines)
OECD	Organisation for Economic Co-operation and Development
PDP	Personal data protection (Vietnam)
SEAMEO	Southeast Asian Ministers of Education Organization
SEAMEO INNOTECH	SEAMEO Regional Centre for Educational Innovation and Technology
T&Cs	Terms and conditions
UN-OHCHR	Office of the United Nations High Commissioner for Human Rights

1. Introduction

Across Southeast Asia, Artificial Intelligence (AI) is increasingly being integrated into education systems (↑Pannen et al., 2025). In parallel, concerns about the safe and responsible use of AI have prompted guidelines and policies to ensure that this technology supports equitable, transparent, and accountable learning environments (↑ASEAN Secretariat, 2024). Such considerations stem from a recognition of the serious and far-reaching consequences of weak data privacy practices and an understanding that AI can magnify these risks further. For example, one well-documented issue in the EdTech space is the oversharing of children's personal data with third parties for commercial purposes (↑Hooper et al., 2022). A potential consequence of this is the targeted advertising and profiling of children, which can limit their potential and self-development as behavioural predictions influence options and choices throughout childhood and even into adulthood (↑Cannataci, 2021). The embedding of AI into EdTech services is usually accompanied by the collection of vast amounts of student data, often including information about behaviour, ability, or even emotion, which exacerbates these risks (↑Holmes, 2025). Another example is that of algorithmic bias, which can lead to unjust outcomes for children from certain groups by replicating stereotypes and biases in their training data, thereby perpetuating social inequalities (↑Kolkman, 2020).

National and regional policies, guidelines, and laws have emerged to address these privacy concerns (↑Paulger, 2023), but the question of how effectively they are implemented in practice remains open. A large part of the answer lies in understanding private EdTech providers, who play a critical role in operationalising these regional and national ethical commitments, as they have the closest interaction with end users (↑Day et al., 2025). Learners and educators experience these commitments not through high-level policy documents, but through the providers' operational practices, such as their terms and conditions (T&Cs) and privacy policies. These policies define how data is collected, processed and shared, and delineate the limits of accountability in AI-enabled learning environments. It is therefore vital to understand how successfully providers are aligning these practices with high-level ethical commitments on trust, child protection, transparency, and accountability.

In this brief, we aim to answer the question:

To what extent are private EdTech companies aligning with national and regional ethical commitments for the safe and responsible implementation of AI in education?

By analysing the terms and conditions and privacy policies of private EdTech companies against national legislation and ASEAN-level guidance from the Association of Southeast Asian Nations (↑ASEAN Secretariat, 2024), the brief seeks to assess whether concerns around trust, child protection, transparency, and accountability are being addressed in practice and where significant gaps remain.

In doing so, the brief contributes to ASEAN's broader efforts to strengthen ethical governance of AI in education, supporting innovation that protects learners' rights, builds trust, and advances inclusive and sustainable digital transformation (↑ASEAN Secretariat, 2024).

2. What stakeholders are calling for

Recent analytical work supported by EdTech Hub, including regional engagement led by SEAMEO INNOTECH (the Southeast Asian Ministers of Education Organization's Regional Centre for Educational Innovation and Technology) on AI readiness and workforce development, highlights both the growing momentum around AI adoption in education and the governance challenges that accompany it. Consultations with ministries of education, educators, SEAMEO centres, private providers, and international organisations revealed a recurring concern: while interest in AI-enabled education is accelerating, ethical safeguards, data governance arrangements, and institutional accountability mechanisms are not always keeping pace. These concerns are echoed in the literature with a report from the International Centre for Higher Education Innovation raising "critical ethical concerns, including data privacy, algorithmic bias, and potential misuse" and recommending "robust ethical guidelines and policies [...] to mitigate risks and ensure AI technologies are used responsibly in higher education in Southeast Asia" (↑Pannen et al., 2025, p. 36).

The aforementioned work with SEAMEO INNOTECH highlights a shared recognition of AI's potential in education, alongside growing concern about how ethical risks are being managed in practice. While perspectives vary across stakeholder groups, there is broad agreement on the need for clearer safeguards, stronger accountability, and more practical guidance to support the responsible adoption of AI in education.

Table 1 below summarises key ethical concerns and suggestions raised across stakeholder groups, which inform the analytical focus of this brief.

Table 1. *Key concerns of education stakeholders regarding ethical safeguards and data governance related to the use of AI in education*

Stakeholder group	Key ethical concerns	What stakeholders are calling for
Ministries of education	Lack of education-specific ethical standards, unclear accountability for AI use and risks to system governance.	Clearer guidance on responsible AI use in education, including the roles and responsibilities of public and private actors.
Educators and schools	Limited capacity to assess AI outputs, risks of overreliance on AI and data protection concerns.	Practical guidance and support to help educators use AI safely, responsibly, and with professional judgement.
SEAMEO centres	Uneven readiness across systems, cybersecurity risks, and limited operational guidance.	Context-specific, actionable frameworks that translate ethical principles into implementable practices.
International organisations	Child protection, learner rights, bias and exclusion, unsafe data practices.	Stronger safeguards for children and vulnerable learners, with explicit attention to consent, data use, and profiling.
Private EdTech providers	Regulatory fragmentation, uncertainty around ethical expectations, and compliance challenges.	Clearer and more consistent standards, particularly on data governance, consent, and child protection, to support ethical innovation.

In light of stakeholder calls for clearer safeguards, stronger accountability, and greater transparency in the use of AI in education, this brief focuses on how ethical and regulatory expectations are reflected at the point where learners and educators most directly encounter them.

3. Analytical focus and rationale

This brief adopts the terms and conditions and privacy policies of private companies as its primary data source. These documents function as formal governance instruments that EdTech providers use to define permissible use, data practices, consent mechanisms, and the limits of their responsibility. As such, they provide a consistent and comparable basis for examining how ethical and legal expectations are articulated at the company level. Beyond assessing alignment with national regulatory frameworks, the analysis applies a secondary, regional lens by comparing company policies against the ASEAN Guiding Principles on AI Governance and Ethics (↑ASEAN Secretariat, 2024). This enables examination of whether and how regionally agreed ethical principles are reflected in standardised company documentation.

This analytical approach was applied to a sample of private EdTech companies operating in Vietnam and the Philippines to focus our investigation. The rationale for the company and country criteria for our sample is given in Section 4.2.

Note that this analytical approach does not assess implementation in practice. Rather, it examines the extent to which national and regional ethical commitments related to child protection, data governance, transparency, and automated processing are formally reflected in the company policies.

4. Methodology

This brief addresses the following research questions:

- How do EdTech companies in Vietnam and the Philippines reflect ethical requirements stated in national frameworks relating to AI in their terms and conditions (T&Cs) and privacy policies?
- How closely do company policies align with the ASEAN Guiding Principles on AI Governance and Ethics?

4.1. Approach

This brief draws on a structured, desk-based analysis of global and regional best practices and standards, followed by a review of publicly available terms and conditions and privacy policies from learner-facing EdTech companies in Southeast Asia. The analysis examines how ethical considerations are articulated in company documentation, with reference to national legislation and ASEAN-level governance principles.

4.2. Country selection and justification

A regional feasibility scan of EdTech companies across Southeast Asia was conducted using structured internet searches (supplemented by EdTech directories) to assess whether sufficient publicly accessible documentation was available for review. For the purposes of this brief, 'feasibility' meant being able to identify multiple learner-facing companies in a given country that (i) operate in or are headquartered in that country and (ii) publish at minimum a publicly accessible privacy policy and/or terms and conditions that could be reviewed without registration. Countries where this threshold was consistently met and documentation contained enough detail to support ethical analysis (e.g., beyond a short boilerplate notice), were prioritised.

Singapore and Malaysia, although well regulated, were excluded to avoid bias towards more mature governance contexts (↑Allen et al., 2025; ↑UNESCO, 2025). Several lower-income countries were also excluded due to limited or absent policy documentation among EdTech companies based in those regions.

Vietnam and the Philippines were selected as lower-middle-income contexts where the feasibility threshold was met and where there was sufficient publicly accessible policy material to support document-based ethical assessment. ↑Honda et al. (2024) and ↑Jayasinghe et al. (2025) describe Vietnam as a context with a growing and diverse EdTech ecosystem, with learner-facing platforms and applications gaining traction alongside increased policy attention to digital learning. The Philippines was selected because the feasibility scan identified multiple learner-facing platforms with sufficiently detailed public terms and conditions and privacy policies to enable comparative analysis, and because there is clear evidence of growing institutional engagement with AI in education, including the Department of Education's establishment of the Education Center for AI Research (E-CAIR) (↑Department of Education, 2025). Together, the two countries enable examination of provider practice in settings with similar income positioning, while differing in market structure and governance context, in ways that are relevant to the ethical risks assessed in this brief.

4.2.1. Company identification and sampling

Approximately 20 companies in each of the two countries were identified through web searches, EdTech directories, and ChatGPT-assisted discovery. From this initial pool, companies were included if they:

- serve school-aged learners or youth directly;
- are headquartered in Vietnam or the Philippines;
- provide links to publicly published terms and conditions and/or privacy policies;
- provide a service or product that demonstrates relevance to data governance and/or ethical considerations (including, but not limited to, virtual learning chatbots, adaptive learning systems, or tutoring solutions involving EdTech and virtual delivery elements).

Transnational providers were excluded. In order to mitigate potential language issues, AI tools such as DeepL and Gemini were used to support translation to assess the appropriateness of the selected company, preventing language from becoming a mitigating factor.

Only four companies from the Philippines met our criteria, and all were included in our analysis. Vietnam had a greater number of suitable companies; however, to ensure balance in our overall sample, we randomly selected four from the eligible pool in Vietnam (see Table 2 below).

Table 2. *Final sample of companies selected for analysis*

Country	Companies included	Notes
Vietnam	4	Selected at random from the eligible set, of which two deeply embedded AI into their services.
Philippines	4	All eligible companies with sufficient documentation that meet eligibility criteria.

4.3. Analytical framework

Company policies were analysed using a structured coding framework to assess how learner-facing EdTech providers describe privacy, security, and governance safeguards in publicly available terms and conditions and privacy documentation. The aim was to support consistent comparison across providers and to identify where policy language is specific and enforceable, where it is incomplete, and where key safeguards are missing.

Benchmarks: Policies were assessed primarily against the national data protection frameworks in each country: in Vietnam, Decree No. 13/2023/ND-CP on Personal Data Protection (PDP)(↑thuvienphapluat.vn, 2023); and in the Philippines, the Data Privacy Act of 2012 (DPA) (↑NPC, 2011) and the National Privacy Commission's 2024 Guidelines on Child-Oriented Transparency (NPC guidelines) (↑NPC, 2024). The ASEAN Guiding Principles on AI Governance and Ethics served as a secondary reference point to inform the interpretation of AI-related transparency and accountability expectations in the narrative analysis.

Coding categories: Coding was organised across seven categories:

1. Age and consent
2. Data collection and minimisation
3. Use of AI and automated decision-making
4. Children's rights and transparency
5. Data retention and security
6. Data sharing and cross-border transfers
7. Design and harm reduction.

Within each category, the analysis focused on whether policies set out the practical elements needed to operationalise safeguards, such as stated thresholds, defined processes, and clear responsibilities, rather than relying on broad commitments.

Country-specific interpretation: Where legal definitions and thresholds differ between Vietnam and the Philippines, each company was assessed against the requirements applicable in its operating context. In Section 5 on findings, which follows, each thematic subsection begins by stating the relevant legal expectation at a level sufficient to interpret company provisions, and then specifies the core indicators used to assess alignment.

Recording alignment: Levels of alignment were recorded as 'aligned', 'partially aligned', or 'not aligned', with brief analytical notes retained to document the rationale for each classification. In general, 'aligned' indicates a clear and actionable policy commitment consistent with the relevant requirement; 'partially aligned' indicates incomplete coverage or non-specific statements; and 'not aligned' indicates omission, contradiction, or provisions that are inadequate for the level of risk.

4.4. Limitations

- The small sample size limits generalisability, as the analysis provides a snapshot of company policy at a specific point in time rather than a comprehensive or longitudinal review of the EdTech sector. Companies were selected to reflect a range of models and contexts, and findings are therefore intended to highlight emerging patterns and risks rather than draw definitive conclusions.

- Transparency bias affects countries and companies lacking published policies, as only providers with publicly accessible terms and conditions and privacy policies could be included in the analysis. This may exclude companies with weaker governance practices from review, while also highlighting a broader accountability gap where the absence of published policies limits user awareness and regulatory scrutiny. This constraint was more pronounced in the Philippines sample and is discussed further in Section 5.4.1.

- Language differences may influence interpretation, particularly where company policies were not originally drafted in English and legal or technical terminology does not translate directly. To mitigate this, ambiguous provisions were interpreted cautiously and coded only where meaning was sufficiently clear, avoiding assumptions about intent or practice where wording was unclear.

- Policies represent a single moment in time and may change, as the analysis reflects the versions of company policies available during the review period (August–December 2025). Subsequent updates or revisions made after this period are not captured, and findings should therefore be understood as time-bound.

4.5. Ethical considerations

All material used was publicly accessible. No human participants were involved. Company names were anonymised during comparative synthesis. Insights are intended to support regionally applicable, responsible governance approaches, rather than assign blame or wrongdoing.

5. Findings

The findings are presented in two complementary formats. Table 3 and Table 4 summarise how companies from Vietnam and the Philippines align or do not align with key requirements of their respective national data protection frameworks based on their publicly available data privacy policies. Second, the narrative findings that follow present both cross-country and country-specific strengths and weaknesses in policy alignment. Drawing on policy excerpts and national requirements, they explain how the gaps identified in company documentation may affect learner protection, with a focus on child safeguards, security, breach response, third-party data sharing, and transparency on automated processing.

5.1. Country Snapshots

Table 3 *Snapshot of how EdTech providers in Vietnam align or do not align with key national data protection requirements*

Ambiguity and overreach	■ Vague on which third parties receive data. ■ Some companies explicitly mention sharing data for marketing or ad optimisation. ■ Often collect more data than necessary (e.g., browser, location, and device data).
Weak child protection practices	■ Little to no detail on age verification. ■ Age thresholds are sometimes not mentioned. ■ AI-related consent and the use of sensitive data (such as voice recordings) are often not well addressed.
Security and accountability	■ Strong on technical encryption measures. ■ Weak on human safeguards — staff training, audits, or oversight. ■ Breach disclosures are vague — none clearly mentions the 72-hour rule[1].
Lack of AI-specific policies	■ Missing explanations on key safeguards for AI features. ■ Missing explanations on how issues such as algorithmic bias are avoided. ■ Missing explanations on human oversight or an appeal mechanism for high-impact AI decisions. ■ Missing evidence that a Data Protection Impact Assessment or high-risk assessment has been done.
Positive Practices	■ Transparency about data collected. ■ Retention periods mentioned. ■ Option to withdraw/delete personal data is clearly explained. ■ For the most part, data appears to be shared appropriately with relevant or necessary third parties.

[1] Article 23.1 of the DPA states that a data breach must be disclosed no later than 72 hours after the violation occurs (↑thuvienphapluat.vn, 2023).

Table 4 *Snapshot of how EdTech providers in the Philippines align or do not align with key national data protection requirements*

Lacking breadth and depth	■ Policies are generally short and less comprehensive, often failing to address many of the national requirements. ■ Some companies, including 'government-backed' ones, do not have privacy policies.
Weak child protection practices	■ Little to no detail on age verification methodology. ■ None specifically states the age thresholds when determining if someone is a minor. ■ No statement explicitly stating that children's data does not get sold, or that children will not receive behavioural advertising.
Security and accountability	■ No defined deletion or retention periods for data collected. ■ No information about data breach protocols. ■ Security often misses details on encryption methods, access control, and auditing.
Lack of AI-specific policies	■ AI use is limited in the companies analysed, but those that do use it make no mention of it in their privacy policy.
Positive practices	■ Clear identification of the collected data and its purpose. ■ No evidence of overreach or collecting information beyond what is required to provide the service. ■ No mention of sale or misuse of data to third parties. ■ The rights to delete and correct personal data are clearly described.

5.2. Cross-country themes

Across Vietnam and the Philippines, the analysis identified a common pattern of partial compliance with national data protection requirements among learner-facing EdTech providers. While most companies demonstrate baseline awareness of data protection obligations, significant ethical and governance gaps remain in how risks are addressed in company terms and conditions and privacy policies.

Some cross-cutting weaknesses that emerged across both countries were:

- Weak child protection practices
- Gaps in security and accountability measures
- Absence of AI-specific transparency and safeguards.

5.2.1. Weak child protection practices

Child protection, for the purposes of this analysis, refers to policies governing the collection and processing of children's personal data. These requirements operate in addition to general data protection obligations and are subject to heightened safeguards under national law.

Under Vietnam's Personal Data Protection Decree (PDP), the processing of children's personal data from the age of seven requires consent from both the child and their parent or guardian, and age must be verified prior to processing (↑thuvienphapluat.vn, 2023). The Philippines' Data Privacy Act (DPA) similarly indicates that reliance on user self-declaration alone may be inadequate for high-risk processing activities (↑NPC, 2011), a position reinforced by the National Privacy Commission's Guidelines on Child-Oriented Transparency (↑NPC, 2024).

Against this legal framework, the analysis assessed two core indicators:

1. whether age verification is conducted beyond user self-declaration;
2. whether consent from both children and their parents or guardians is explicitly required.

Across both countries, weak child protection practices emerged as a consistent cross-cutting issue. Only three of the eight companies reviewed specify an age threshold for defining a child in their policies. Just two providers describe any form of age verification practice. Several companies appeared to rely entirely on trust-based self-declaration; for example, Company X has the following to say regarding age declaration in their privacy policy:

> *If you are opening an account on behalf of yourself, you represent that you are the age of majority in your jurisdiction and fully able and competent to enter into these Terms.*

Such provisions do not meet the child protection standards set out in either national framework.

Weak age-verification practices increase the likelihood that children's personal data may be collected, processed, or shared without appropriate safeguards, including parental oversight or consent. Without parental involvement, preventative measures such as informed consent, supervision of data use, and the ability to exercise data rights on a child's behalf are less likely to be in place. Once shared with third parties, control over data retention and secondary use becomes significantly more difficult. Children may also be exposed to behavioural profiling, targeted advertising, or commercial exploitation of their data. In the event of data breaches, risks are further heightened, including potential location tracking, contact by harmful actors, and unintended disclosure of personal content (↑ICO, 2024b).

5.2.2. Security and accountability

For the purposes of this analysis, security and accountability refer to the technical and organisational measures put in place to protect personal data from unauthorised access, loss, or misuse, and to ensure a timely and appropriate response when data protection violations occur. Under Vietnam's Personal Data Protection Decree (PDP), organisations are required to implement both technical and organisational safeguards, including measures to prevent unauthorised access and clear procedures for responding to data protection violations (↑thuvienphapluat.vn, 2023). The PDP further requires notification of personal data breaches within 72 hours of detection. A data breach is any security incident in which unauthorised parties access sensitive or confidential information, including personal data (↑Kosinski, 2025). The Philippines' Data Privacy Act (DPA) similarly mandates reasonable and appropriate security measures and states that notification to affected parties should not be delayed beyond what is necessary (↑NPC, 2011).

Against this framework, the analysis examined two core dimensions:

1. The presence of technical and organisational security measures.
2. The clarity of accountability and breach notification procedures.

Across both countries, most companies demonstrate relatively strong attention to technical safeguards. Six of the eight providers reviewed describe industry-standard technical security measures, such as encryption and access controls, consistent with baseline requirements under the PDP and DPA.

However, organisational safeguards are far less consistently addressed. Only three providers mention practices such as staff training, internal audits, or define roles and responsibilities for data protection. This represents a notable gap, given that many data breaches result from human error, misconfiguration, or social engineering rather than purely technical failure (↑Mimecast, 2025).

Accountability mechanisms in the event of data breaches are also weak. Six of the eight providers do not specify any breach notification protocol in their policies. The two providers that do, include only vague commitments, for example:

> *If a data breach occurs, [Company X] will notify affected parties and work with authorities to resolve the issue promptly.*
>
> *In case the server storing information is hacked, leading to the loss of customer personal data, [Company Y] will be responsible for reporting the incident to the authorities for timely investigation and notification to the customer.*

Such imprecise language provides significant discretion to delay notification and does not clearly reflect the timelines or expectations set out in national law. Delayed notification can prevent users from taking timely protective actions, such as changing passwords or cancelling payment cards, and may extend the period during which compromised data can be misused (↑Dimov, 2018). Where contact or location data is involved, delayed disclosure can also expose individuals to real-world risks, including harassment or physical harm.

5.2.3. Lack of AI-specific policies and disclosures

It is notable that neither Vietnam's Personal Data Protection Decree (PDP) nor the Philippines' Data Privacy Act (DPA) contains provisions explicitly related to Artificial Intelligence (↑NPC, 2011; ↑thuvienphapluat.vn, 2023). Comprehensive laws and regulations specifically addressing AI-related concerns are not yet in force in Vietnam or the Philippines, but they are being developed actively. Vietnam has drafted and adopted a new Law of Artificial Intelligence that will set out requirements regarding "transparency, accountability, and security throughout the lifecycle of AI systems" (↑Ministry of Science and Technology, 2025b), which will come into force on 1 March 2026. The Philippines does not yet have a standalone AI law, but its NPC guidelines outline several key AI safety principles.

However, both the DPD and the DPA currently specify regulations on automated processing and profiling of personal data. These are defined as forms of electronic processing used to evaluate, analyse, or predict aspects of an individual's behaviour, preferences, location, abilities, or other characteristics. Under both frameworks, such processing and its purposes should be disclosed to users as part of transparency and informed consent requirements. This regulatory framework is particularly relevant to AI-enabled education tools, where interactions frequently involve text, audio, images, or video that may contain personal or sensitive information. A subtle yet crucial concern is algorithmic bias. It is well understood that AI can replicate stereotypes and biases contained in its training data (↑Kolkman, 2020), which is particularly concerning when AI is used to predict learning trajectories, capacities, and outcomes (↑Day et al., 2025). Learnt biases with respect to gender, race, and culture may therefore influence learning pathways, feedback, or assessment, leading to unfair outcomes for already marginalised children.

Despite these regulations on automated personal data processing and profiling, the analysis revealed a complete absence of disclosures about AI uses across the sample. None of the eight companies reviewed explicitly state whether AI is used in the processing of user data, nor do they describe AI-related risks, safeguards, or data governance practices in their terms and conditions or privacy policies. This includes providers that publicly market their products as AI-enabled in promotional materials. The absence of AI-specific policy language represents a significant transparency and accountability gap. Without clear disclosure, users cannot understand whether automated processing or profiling is occurring, what types of data may be involved, or what safeguards are in place, thereby limiting the legal validity of any consent provided by children.

5.2.4. Positive practices and emerging foundations

Despite identified gaps in child protection, security and accountability, and AI-specific transparency, several companies demonstrate positive foundations that could be strengthened over time; examples of good practice across both countries include the clear articulation of users' rights to access, modify, or delete their personal data held by the provider, evidence of technical safeguards such as encryption to protect stored and transmitted data, and evidence of impact assessments or safeguards related to cross-border transfers of personal data, all of which indicate that some providers are taking steps towards stronger data governance.

5.3. Country-specific findings: Vietnam

While the cross-country analysis highlights shared strengths and weaknesses across Vietnam and the Philippines, certain ethical and governance risks emerge more clearly when examined within specific national contexts. The following Vietnam-specific findings illustrate how ambiguity in company policies can interact with national regulatory requirements in ways that undermine ethical intent and increase risk in practice.

5.3.1. Ambiguity and overreach in data collection and use

Vietnam's Personal Data Protection Decree (PDP) specifies that personal data collected must be appropriate and limited to what is necessary for the service being provided, and that personal data may not be bought or sold (↑thuvienphapluat.vn, 2023)). The PDP further states that consent is only valid if the data subject is informed of the types of data collected, the purpose of processing, and all third parties involved (Article 11.2). When company privacy policies were assessed against these requirements, a recurring pattern of ambiguity emerged. Many policies rely on broad or imprecise language, making it difficult to determine whether data minimisation and informed consent requirements are being met. This ambiguity is particularly evident in descriptions of the types of data collected, the purposes for which data is processed, and the roles of third parties receiving user data.

In some cases, the analysis identified language that appears to go beyond ambiguity and into potential non-compliance. For example, one EdTech provider states that it collects data on:

> [...] *presumed or identified needs, preferences, attributes and insights relevant to our potential or existing engagement, purchasing details including interest and or purchase history, [and] commercial information.*

The same company's privacy policy further declares that the company has:

> [...] *sold or shared Internet or other electronic network activity information, geolocation data, and commercial information, or used personal information for targeted advertising.*

This language suggests the collection and commercial use of personal data that extend beyond what would reasonably be required to deliver an educational service, alongside an explicit acknowledgement of data sale or sharing. Such practices are inconsistent with the PDP's requirements on data minimisation and restrictions on the sale of personal data. More broadly, the prevalence of vague and expansive data collection clauses increases ethical and practical risks for users. Collecting data beyond what is necessary expands the volume of personal information held by providers, increasing exposure in the event of data breaches, and heightening the risk of identity theft, fraud, and misuse. This is especially concerning given that the education sector is frequently targeted by cyberattacks (↑Day et al., 2025), accounting for 5% of ransomware attacks globally (↑APWG, 2022).

5.4. Philippines-specific themes

The following Philippines-specific findings indicate gaps in the breadth and depth of privacy policy documentation, raising concerns about transparency in data processing. These gaps are particularly acute in privacy documentation accessible by children.

5.4.1. Limited transparency and thin policy documentation

Compared with companies in Vietnam, companies in the Philippines sample tend to publish shorter and less detailed privacy documentation. Several learner-facing platforms identified in the initial scan do not provide accessible public privacy policies or terms and conditions, which meant they could not be included in the analysis. As a result, the pool of eligible companies was smaller, and the four providers in the Philippines analysed for this study were the only companies identified out of 20 that met the inclusion criteria and had sufficient documentation for review.

This has two implications. First, it introduces an additional methodological limitation, as it reduces the ability to sample from a wider set of comparable providers. Second, it raises compliance and enforcement concerns. Under the Philippines' Data Privacy Act (DPA), organisations are expected to provide clear transparency about how personal data is collected and processed (↑NPC, 2011). The absence of publicly accessible privacy information suggests potential gaps in the practical enforcement of data protection requirements for some private providers.

5.4.2. Lack of child-oriented transparency

A second theme that emerged relates to child-oriented transparency. Privacy policies are often written in legal or technical language that is difficult for most users to interpret, particularly for children. The National Privacy Commission's Guidelines on Child-Oriented Transparency recommend providing age-appropriate notices that explain data practices in clear, plain language, while retaining essential concepts in a manner comprehensible to children (↑NPC, 2024). Our analysis, however, found that none of the four private providers reviewed in the Philippines publishes an age-appropriate version of their privacy policy. This represents a clear gap against recommended practice and may weaken meaningful consent for child users. Where children cannot understand what data is being collected, how it is used, and when it may be shared, consent becomes more formal than informed. This also limits children's ability to exercise key data subject rights in practice, including the rights to access, correct, or delete their information, and to raise concerns or complaints.

5.4.3. Positive practices

Despite these gaps, the Philippines sample also demonstrates several strengths in privacy policy content. Providers tend to describe the categories of data collected and the purpose of collection with relatively high clarity. Several policies also specify retention periods that align with regulatory expectations. Where third-party data sharing is described, it is generally limited to relevant or necessary parties, suggesting comparatively stronger restraint in disclosure.

5.5. Secondary analysis: Alignment with ASEAN AI Governance and Ethics Principles

The ASEAN Guiding Principles on AI Governance and Ethics provide a shared regional reference point for responsible, human-centred, and accountable use of AI (↑ASEAN Secretariat, 2024). When company policies are mapped against these principles, several recurring gaps emerge across both country samples. These gaps appear consistent regardless of whether platforms are explicitly AI-enabled, suggesting that ethical governance is not quite yet in step with technological adoption in education. While there is overlap between the ASEAN principles and national data protection frameworks in both Vietnam and the Philippines, similar shortcomings were observed, indicating persistent gaps between regulatory intent and company practice.

Across both countries, some policies include baseline elements that partially align with ASEAN's Principle 6 on privacy and data governance, including disclosure of basic data categories collected, user rights, such as deletion or withdrawal of consent in some cases, and general security commitments. A small number of providers also include child-focused measures such as parental guidance, parental controls, or ad-free design. However, these practices are uneven and rarely extend to AI-specific transparency, accountability, or fairness safeguards.

Areas of non-alignment with ASEAN's principles are outlined thematically in the subsections below.

5.5.1. Parental consent and age verification (Principles 5 and 6)

Across Vietnam and the Philippines, parental consent and age verification are inconsistently reflected in companies' terms and conditions and privacy policies. Only one provider described a sign-up process that effectively verifies parental involvement through parent registration. A small number of providers reference parental consent in principle, but do not describe how it is verified. Several platforms rely on exclusionary statements declaring that services are not intended for minors and that they will delete children's data if discovered, rather than establishing proactive safeguards. Overall, most services fall short of expected regional legal and ethical standards for processing children's data, a situation that is particularly concerning in educational contexts. Weak consent and age-verification practices reduce parents' visibility and control over how their children engage with digital learning tools, making it harder to identify risks, raise concerns, or intervene when data is misused or shared beyond the educational purpose.

5.5.2. Transparency on AI use and automated processing (Principle 1)

Company policies rarely disclose clearly whether AI or automated systems are used, what they are used for, or what kinds of data they process. Some policies reference automation through personalisation or analysis of user activity, or imply automated processing through the collection of user-generated content such as prompts, audio, images, or video. However, these references are generally not framed in terms of AI use and do not explain how automated processes affect learners. None of the reviewed policies provides accessible explanations of automated decisions, their impacts, or routes to challenge outcomes.

5.5.3. Accountability and breach response procedures (Principle 7; Principle 3)

Most providers include general statements about security, and some reference technical safeguards such as encryption or access controls. However, breach notification procedures are frequently missing or vague. Some policies rely on user-initiated reporting rather than clearly stating the provider's obligation to notify users in the event of a breach, and timelines are often unspecified. Accountability for data shared with third parties is also often unclear, with limited clarity about who remains responsible after disclosure to vendors or partners.

5.5.4. Fairness, bias safeguards, and harm reduction (Principle 2)

Across both samples, there is little evidence in company policies of safeguards against discriminatory or biased outcomes or of commitments to monitor and mitigate harm, including internal oversight structures, such as ethics committees, risk boards, or regular reviews. Policies rarely mention testing for the accuracy, reliability, or resilience of automated systems, and none describes independent audits or third-party reviews of AI-related risks.

5.5.5. Sustainability and societal well-being (additional consideration)

References to sustainability, environmental impacts, or broader societal well-being are entirely absent across both country samples.

5.5.6. Summary

Overall, EdTech companies across Vietnam and the Philippines exhibit significant, cross-cutting gaps in how they address privacy and security, most notably regarding child safety and protection. Weak child protection practices are widespread, as most EdTech providers rely on children's self-declaration of age or parental trust-based consent, methods that fail to meet the legal requirements for age verification and informed consent set by the national frameworks of both countries. If parents are not kept in the loop, it increases the risk that children will be exposed to content that is not appropriate for their age. This inadequacy is further compounded by a lack of child-oriented transparency, where complex, legalistic privacy policies are inaccessible to school-aged children, thus undermining the possibility of 'meaningful consent'. Crucially, all but one of the companies provide AI-specific disclosures, leaving parents and learners unaware of whether and how automated processing or profiling, which often involves sensitive data like voice recordings, is being used with children's data. Furthermore, in Vietnam, findings revealed overreach in data collection, including the collection of information beyond what is necessary (e.g., location data), and the explicit acknowledgement by one provider of having "sold or shared" personal information for targeted advertising. Collectively, these gaps in consent, transparency, and accountability are compounded by weak security and breach notification protocols— where most providers lack a clear policy for timely breach disclosure—all of which severely limit parental oversight and control, heightening the risk of children's data being misused, sold, or exposed in a data breach.

Beyond the obvious risks outlined above, these issues can also affect and influence children's learning outcomes. A lack of clear policies on AI use, specifically regarding safeguards against algorithmic bias, may lead to discriminatory outcomes that limit a child's educational opportunities or mislead children with inaccurate or biased feedback, undermining the goal of an equitable learning environment. Targeted advertising and profiling expose children to distractions and commercial pressures, which can reduce their ability to focus and engage fully with their education (↑Cannataci, 2021). A more systemic concern is the erosion of trust stemming from issues related to data privacy and the protection of guardians' and educators' information. Guardians may be reluctant to consent to the use of a tool, and schools may be wary of adopting EdTech solutions due to governance and liability concerns, hindering the equitable adoption of effective EdTech for all learners.

6. Recommendations

This section presents recommendations to strengthen the ethical governance of AI in education in Southeast Asia. While regional and national frameworks articulate important values, this review indicates that ethical governance will not improve through principles alone. Learners and educators experience safeguards through everyday practices in classrooms, schools, and homes. Progress, therefore, requires coordinated action across regional bodies, national regulators, ministries of education, and private EdTech providers, with a focus on transparency, child protection, accountability, and practical implementation at the point of use.

6.1. Support teachers and parents to enable safe and responsible AI use for learners

Learners encounter AI-enabled tools primarily through classroom activities and home use, making teachers and parents critical intermediaries in ensuring safe and responsible engagement. UNESCO's guidance on generative AI in education stresses that real-world safeguards depend on practical implementation and human capacity in education systems, not only on high-level principles (↑Miao & Holmes, 2023). Ethical risks, including unclear data use, automated feedback that may be misleading or inappropriate, and exposure to harmful content, are therefore often mediated through everyday pedagogy and supervision in children's environments. UNICEF similarly frames child-centred AI as requiring protections and enabling conditions around children in practice, including in the settings where they learn and live (↑Day et al., 2025).

To operationalise these safeguards at the point of use, **ministries of education should integrate AI ethics, child data protection, and safety considerations into continuous professional development for teachers.** Training should equip educators not only to use digital tools effectively, but also to explain when AI-enabled features are in use, what data may be collected, what outputs or decisions are automated, and what safeguards and escalation routes are in place. In practice, several systems are already moving in this direction, for example, through ministry-led guidance and resources, including Australia's national framework for generative AI in schools and New South Wales's parent-facing materials to help families understand AI use in education.

Teacher training institutions and schools should embed responsible AI use, data protection, and child safety into in-service training and coaching. Schools can use existing channels, such as parent–teacher meetings and routine school communications, to explain which learning platforms are used, what they do, what protections apply, and how concerns can be raised. This aligns with regulatory expectations that child-facing services provide privacy information in formats that are accessible to children, parents, and carers (↑ICO, 2024b). As an example of practical best practice, Australia's eSafety Commissioner provides free webinars for parents and carers that address emerging AI risks and offer concrete supervision strategies families can use at home, including a dedicated session on 'AI companions' that provides practical tools and signs to look out for (↑eSafety Commissioner, 2025)

EdTech providers should offer clear, accessible guidance for teachers and parents on how their tools use AI and learner data, including plain-language explanations of automated features, safety controls, and reporting pathways. This is consistent with ASEAN guidance emphasising transparency and the value of sharing information about AI use and data practices in ways that are useful and understandable to users.

6.2. Establish minimum safeguards for learner-facing AI and digital tools

In the samples from Vietnam and the Philippines, high-level ethical and legal principles are not consistently reflected in company policies, particularly regarding children. In education settings, reactive measures such as deleting data once a child is identified fall short of expectations that protections should be designed in from the outset, including through "data protection by design and by default" in services likely to be accessed by children (↑ICO, 2024b).

Regional bodies should support the development of a simple, education-specific checklist of minimum safeguards for learner-facing AI and digital tools, to translate regional principles into practical requirements. This can be led by ministries of education and supported by regional bodies through model templates and shared good practice. Drawing on UNICEF's *Guidance on AI and Children 3.0* checklist, minimum safeguards for education could be framed as a short set of non-negotiables covering child protection, consent and age considerations, transparency on automated processing, third-party data sharing, and incident or breach response (↑UNICEF Innocenti, 2025).

As multiple regional frameworks and guidance documents are under development, it is even more important to ensure regular and visible monitoring in parallel. **National regulators and data protection authorities should strengthen proactive monitoring of learner-facing EdTech platforms against existing legal thresholds, and publish periodic signals on recurring gaps, risks, and emerging good practice.** This would reduce ambiguity for schools and providers, and help shift the sector from reactive compliance towards consistent baseline safeguards.

An additional safeguard is for ministries of education to define non-negotiable minimum conditions for any EdTech platform used in public education. These minimum conditions would set clear expectations for providers and can be operationalised through procurement and endorsement processes. In settings where platform choice is devolved to schools or teachers, ministries can provide a short screening checklist or approved list to help users avoid tools with weak child safeguards, unclear data practices, or opaque automated features.

EdTech providers should implement proactive child protection measures where children are likely users, including age verification and parental involvement where appropriate. Safeguards should prevent unsafe or unlawful processing by default rather than relying solely on exclusion statements or post hoc deletion (↑ICO, 2025a).

6.3. Improve transparency and disclosure of AI use and automated processing

This study finds that AI use and automated processing are rarely clearly explained in company policies, even where such systems shape learning experiences. This lack of transparency limits informed consent, reduces trust, and makes accountability difficult for educators, parents, and learners. Transparency and responsible disclosure are widely recognised as baseline requirements for trustworthy AI, particularly where systems affect people's opportunities and well-being (↑OECD, 2019).

To make disclosure workable in education settings, national regulators and ministries of education should require a short, standard AI disclosure for any learner-facing tool used, procured, or recommended in schools. This disclosure should be completed by providers in plain language and made available alongside or within formal policies. At minimum, it should state whether AI or automated processing is used; what it is used for (for example, feedback, recommendations, content generation, scoring, or progress tracking); what types of learner data it relies on; whether outputs materially shape learning pathways; and what users can do if they have questions or concerns, or wish to raise a complaint. UNESCO's guidance on generative AI in education reinforces the importance of practical, usable transparency measures that education systems can understand and act on (↑Miao & Holmes, 2023).

As AI-enabled features evolve quickly, **national regulators should treat transparency and disclosure guidance for EdTech providers as a 'living' resource, subject to timely review and update when risks, product capabilities, or common compliance gaps change materially**. Regulators should publish versioned updates and clear change notes so schools and providers can track what has shifted over time. One practical example is the UK Information Commissioner's Office, which updated its Guidance on AI and data protection and signposts updates for readers (↑ICO, 2023).

An additional safeguard is for ministries of education to integrate disclosure requirements into onboarding, procurement, or approval processes, and to support schools to interpret disclosures in practice. This includes understanding what automated features do, what data they rely on, what meaningful choices users have, and what escalation routes exist, so schools can communicate effectively with teachers, learners, and families.

EdTech providers should publish a clear, plain-language AI disclosure alongside or within their privacy policies, and ensure it is easy to find at the point of sign-up and use. For child-facing services, disclosures should be accessible to both children and parents or carers, reflecting regulatory expectations that information be presented in forms children can understand, and that support informed oversight by adults (↑ICO, 2025a). Where AI influences learning pathways, content recommendations, feedback, or progress tracking, providers should explain this at a high level and indicate how risks of inappropriate personalisation or bias are monitored and addressed.

6.4. Strengthen accountability, third-party responsibility, and ongoing governance

For learners and families, accountability matters most when something goes wrong. It affects whether harms are prevented, identified early, and dealt with quickly. When products change, but policies do not keep up, and when learner data is shared with third parties, responsibility can become unclear. This can increase child safety risks and make it harder for schools and families to get timely support or remedies. As AI-enabled tools are updated frequently, national regulators should clarify expectations for accountability across vendor and subcontractor chains in EdTech. This should include who is responsible for user protection, who must notify schools and users when a breach occurs, and how responsibilities apply when incidents originate in a supplier environment. Regulators should also reinforce the need for timely breach notification and require documented incident response procedures that remain effective when third parties are involved (↑ICO, 2025b).

An additional safeguard is for ministries of education to designate an accountable owner to regularly review provider compliance over time, rather than treating oversight as a one-off step during procurement. Oversight should remain active throughout the lifecycle of a tool's use in schools. This can include periodic checks and defined triggers for review when products change in ways that may affect learners, such as new AI features, new data flows, or new subcontractors (↑NIST, 2023).

EdTech providers should conduct regular governance reviews of their data and AI practices, including scheduled policy reviews and documented change logs as products evolve. Providers should maintain an up-to-date record of third parties that receive learner data and state clearly which entity remains accountable when data is shared. They should set out breach response procedures and timelines in plain language, including escalation routes for schools and families, and ensure suppliers are contractually required to notify them without undue delay when incidents occur (↑ICO, 2024b). Providers should also adopt structured risk management practices across the AI lifecycle, including clear internal accountability (for example, naming a data protection or compliance lead) and maintaining documentation that supports auditability and supply-chain oversight (↑NIST, 2023; ↑OECD, 2019).

7. Looking ahead

Looking ahead, the core question for education systems in Southeast Asia is not whether AI will be used, but whether it will improve learning in ways that are safe, fair, and trusted. The evidence in this brief suggests the region is still shaping the foundations of AI adoption in education. Choices made now about which tools are introduced, how they are governed, and how they are supported in schools will influence both learning impact and public confidence.

Two findings from this work are particularly relevant. First, the analysis of terms and conditions and privacy policies indicates that many learner-facing providers do not yet translate high-level ethical commitments into clear, operational safeguards. Where child protections, limits on data sharing, transparency about automated features, and routes for accountability are unclear, schools and families are left without practical assurances. This has direct implications for learning. Trust affects whether tools are adopted, how they are used, and whether benefits extend beyond well-resourced users and schools.

Second, the SEAMEO INNOTECH engagement on AI readiness and workforce framework development reinforces a consistent message from stakeholders. Interest in AI-enabled education is accelerating, but institutional arrangements for oversight are uneven. In practice, this means systems risk scaling tools before responsibilities are clear, safeguards are tested in real classroom conditions, and problems can be detected early.

The opportunity, therefore, is to treat ethical governance as an enabling condition for learning impact, rather than as an afterthought once tools are already in use. This requires more than publishing policies. It calls for active monitoring and routine checks throughout the lifecycle of a tool, including clear ownership within ministries and providers, defined triggers for review when products or data flows change, and practical processes for handling complaints, incidents, and redress. Where monitoring is weak, even well-written commitments can remain aspirational.

If governments and providers act now to strengthen safeguards and accountability in ways that are visible to schools and families, AI can be integrated in ways that support safer participation and more equitable learning gains. If they do not, the region risks embedding low-trust practices that limit uptake, concentrate harms among marginalised learners, and undermine the learning benefits AI is intended to support.

Bibliography

This bibliography is available digitally in our evidence library at https://docs.edtechhub.org/lib/2VBH4GZX

Allen, J. G., Loo, J., & Luna, J. (2025). Governing intelligence: Singapore's evolving AI governance framework. *Cambridge Forum on AI: Law and Governance*, *1*, e12. https://doi.org/10.1017/cfl.2024.12. Available from https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/governing-intelligence-singapores-evolving-ai-governance-framework/5E54A373E193E2D51354ADC1F509B9B4. (details)

Anti-Phishing Working Group (APWG). (2022). *Phishing Activity Trends Report 3rd Quarter 2022*. APWG. https://apwg.org/trendsreports. (details)

ASEAN Secretariat. (2024). *ASEAN Guide on AI Governance and Ethics*. ASEAN Secretariat. https://asean.org/book/asean-guide-on-ai-governance-and-ethics/. (details)

Cannataci, J. (2021). *A/HRC/46/37: Artificial intelligence and privacy, and children's privacy - Report of the Special Rapporteur on the right to privacy*. UN Office of the High Commissioner Human Rights (OHCHR). https://www.ohchr.org/en/documents/thematic-reports/ahrc4637-artificial-intelligence-and-privacy-and-childrens-privacy. (details)

Day, E., Byrne, J., & Penagos, M. (2025). *Data Governance for EdTech* [Landscape Review]. UNICEF Innocenti. https://www.unicef.org/innocenti/reports/data-governance-edtech. (details)

Department of Education. (2025, February 20). DepEd launches AI center for education. *Department of Education*. https://www.deped.gov.ph/2025/02/20/deped-launches-ai-center-for-education/. (details)

Dimov, D. (2018, February 17). *Consequences of the late announcement of cyber-security incidents*. Infosec Institute. Available from https://www.infosecinstitute.com/resources/incident-response-resources/consequences-late-announcement-cyber-security-incidents/. (details) eSafety Commissioner. (2025, October 12). *Understanding AI Companions: What parents and carers need to know*. https://www.esafety.gov.au/parents/webinars/understanding-ai-companions-what-parents-and-carers-need-to-know. (details)

Holmes, W. (2025). AI, education, and children's rights. *Frontiers in Education*, *10*. https://doi.org/10.3389/feduc.2025.1656736. Available from https://www.frontiersin.org/journals/education/articles/10.3389/feduc.2025.1656736/full. (details)

Honda, D., Halla, K., Thang, S., & Mazari, H. (2024). *Summary: EdTech in Vietnam - A Rapid Scan*. EdTech Hub. https://doi.org/10.53832/edtechhub.1041. Available from https://docs.edtechhub.org/lib/9RCXRV9J. Available under Creative Commons Attribution 4.0 International. (details)

Hooper, L., Livingstone, S., & Pothong, K. (2022). *Problems with Data Governance in UK Schools: The cases of Google Classroom and ClassDojo* [Monograph]. Digital Futures Commission, 5Rights Foundation. https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf. (details)

Information Commissioner's Office (ICO). (2023, March 15). *Guidance on AI and data protection*. ICO. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/. (details)

Information Commissioner's Office (ICO). (2024a, November 19). *Design for meaningful parent or guardian-child interactions*. ICO. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/childrens-code-design-guidance/design-for-meaningful-parent-or-guardian-child-interactions/. (details)

Information Commissioner's Office (ICO). (2024b, August 18). *Children's Code Strategy progress update - August 2024*. ICO. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/children-s-code-strategy-progress-update-august-2024/. (details)

Information Commissioner's Office (ICO). (2025a, October 16). *Data protection by design and default*. ICO. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/data-protection-by-design-and-default/. (details)

Information Commissioner's Office (ICO). (2025b, August 20). *Personal data breaches: A guide*. ICO. https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/. (details)

Jayasinghe, N., Chrisani, A., Honda, D., & Gunawan, C. J. (2025). *EdTech for Marginalised Learners in Southeast Asia: Perspectives from funders and providers on priorities, design, investment, and scaling considerations* [Landscape Analysis]. EdTech Hub. https://doi.org/10.53832/edtechhub.1117. Available from https://docs.edtechhub.org/lib/SB7G3I83. Available under Creative Commons Attribution 4.0 International. (details)

Kolkman, D. (2020, August 26). F**k the algorithm?: What the world can learn from the UK's A-level grading fiasco [Online resource]. *Impact of Social Sciences Blog*. https://blogs.lse.ac.uk/impactofsocialsciences/. (details)

Kosinski, M. (2025). *What is a data breach?* IBM. https://www.ibm.com/think/topics/data-breach. (details)

Miao, F., & Holmes, W. (2023). *Guidance for Generative AI in Education and Research*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000386693. (details)

Mimecast. (2025). *Mimecast Global Threat Intelligence Report 2025 (January to September)*. mimecast. https://www.mimecast.com/resources/ebooks/threat-intelligence-january-june-2025/. (details)

Ministry of Science and Technology. (2025a, November 28). *Dự thảo Luật Trí tuệ nhân tạo: Hành lang pháp lý cho phát triển, bảo đảm an toàn và chủ quyền số q*. Government of Vietnam. Cổng Thông tin điện tử Bộ Khoa học và Công nghệ. https://mst.gov.vn/du-thao-luat-tri-tue-nhan-tao-dat-con-nguoi-o-vi-tri-trung-tam-197251127191513632.htm. (details)

Ministry of Science and Technology. (2025b, November 10). *Quốc hội thông qua Luật Trí tuệ nhân tạo: Hoàn thiện hành lang pháp lý cho kỷ nguyên số*. Government of Vietnam. Cổng Thông tin điện tử Bộ Khoa học và Công nghệ. https://mst.gov.vn/quoc-hoi-thong-qua-luat-tri-tue-nhan-tao-hoan-thien-hanh-lang-phap-ly-cho-ky-nguyen-so-197251210165544671.htm. (details)

National Institute of Standards and Technology (NIST). (2023). *AI Risk Management Framework*. NIST, U.S. Department of Commerce. https://www.nist.gov/itl/ai-risk-management-framework. (details)

National Privacy Commission (NPC). (2011, July 25). *Republic Act 10173 — Data Privacy Act of 2012*. National Privacy Commission. https://privacy.gov.ph/data-privacy-act/. (details)

National Privacy Commission (NPC). (2024). *Guidelines on Child-Oriented Transparency*. https://privacy.gov.ph/wp-content/uploads/2024/12/Advisory-2024.12.17-Guidelines-on-Child-Oriented-Transparency-w-SGD.pdf. (details)

OECD. (2019, May 22). *Recommendation of the Council on Artificial Intelligence*. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449. (details)

Pannen, P., Riyanti, R., & Min, L. (2025). *Understanding Trends, Activities, and Recommendations Regarding AI Integration in Higher Education in Southeast Asia*. UNESCO-ICHEI: International Centre for Higher Education Innovation under the auspices of UNESCO. https://en.ichei.org/en/knowledge/yjbg/. (details)

Paulger, D. (2023). *Navigating Cross-Border Data Transfers in the Asia-Pacific region (APAC): Analyzing legal developments from 2021 to 2023*. Future of Privacy Forum (FPF). https://fpf.org/resource/navigating-cross-border-data-transfers-in-the-asia-pacific-region-apac-analyzing-legal-developments-from-2021-to-2023/. (details)

thuvienphapluat.vn. (2023, April 17). *Nghị định 13/2023/NĐ-CP bảo vệ dữ liệu cá nhân*. Nghị định 13/2023/NĐ-CP bảo vệ dữ liệu cá nhân. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx. (details)

UNESCO. (2025). *Malaysia: artificial intelligence readiness assessment report* [Assessment Report]. UNESCO. Available from https://unesdoc.unesco.org/ark:/48223/pf0000395618?posInSet=1&queryId=896a039b-385b-4a69-9b75-d472126c18ff. (details)

UNICEF Innocenti. (2025). *Guidance on AI and children: Version 3.0 Recommendations for AI policies and systems that uphold child rights*. https://www.unicef.org/innocenti/reports/policy-guidance-ai-children. (details)