JURNAL CITA HUKUM (Indonesian Law Journal)
FSH UIN Syarif Hidayatullah Jakarta
Vol.14 No. 2 (2026), pp. 635-664, DOI: 10.15408/jch.v14i2.53565

# Governing AI in Education: Mapping the Regulatory Gap Between Algorithmic Deployment and Student Data Protection in Asia-Pacific Jurisdictions*

**Jin Zhen,[1] Haniff Ahamat,[2] Xiao Shurui[3]**
Universiti Kebangsaan Malaysia (UKM), Malaysia

10.15408/jch.v14i2.53565

**Abstract**
The rapid deployment of artificial intelligence systems in educational settings across Asia-Pacific jurisdictions has outpaced the development of regulatory frameworks capable of addressing the distinctive risks these systems pose to student data. This article provides a systematic literature review and descriptive comparative institutional analysis of six major regulatory frameworks: the EU General Data Protection Regulation and AI Act, China's Personal Information Protection Law and algorithmic regulation, the ASEAN national PDPA series, the ASEAN Model Contractual Clauses, and the US FERPA/COPPA reference framework, mapping their coverage against the documented realities of AI education deployment. Four structural dimensions of regulatory gap are identified: (1) the absence of educational context-specificity in platform-neutral regulatory designs; (2) a temporal mismatch between dynamic AI system updates and static compliance mechanisms; (3) the fragmentation of cross-border accountability when student data traverses jurisdictional boundaries; and (4) the diffusion of responsibility across multi-actor deployment chains. This article provides the descriptive and empirical foundation for a three-paper research series. It does not propose solutions or normative prescriptions; those normative and design dimensions are addressed in companion work and constitute directions for future research.

**Keywords:** AI in education; EdTech; student data protection; Asia-Pacific; data governance; regulatory gap; GDPR; PIPL; ASEAN; algorithmic accountability

* Received: April 11, 2026; revised: May 21, 2026; accepted: May 29, 2026; Published: June 30, 2026.
1 **Jin Zhen.** Doctoral candidate, Faculty of Law, Universiti Kebangsaan Malaysia (UKM), Bangi, Malaysia. ORCID: https://orcid.org/0009-0006-3502-9446. Corresponding author. Email: p152393@siswa.ukm.edu.my
2 **Haniff Ahamat.** Professor, Doctor, Faculty of Law, Universiti Kebangsaan Malaysia (UKM), Bangi, Malaysia. ORCID: https://orcid.org/0000-0003-4026-3633 Email: haniff@ukm.edu.my
3 **Xiao Shurui.** Faculty of Law, Universiti Kebangsaan Malaysia (UKM), Bangi, Malaysia. ORCID: https://orcid.org/0009-0008-6234-004X Email: p119267@siswa.edu.ukm.my
** Corresponding Author: p152393@siswa.ukm.edu.my

## A. INTRODUCTION

Artificial intelligence systems have been integrated into educational environments across Asia-Pacific at a pace that substantially exceeds the capacity of existing regulatory frameworks to adapt. Intelligent tutoring systems, adaptive learning platforms, AI-powered assessment tools, learning analytics dashboards, and remote proctoring technologies now form part of the institutional infrastructure of schooling from primary through tertiary levels across the region (UNESCO, 2025; ASEAN Foundation, 2026). This accelerating deployment has created what might be described as an institutional vacuum: student data, ranging from basic academic records to real-time biometric streams, is continuously collected, processed, analysed, and in many cases transferred across national borders, yet the legal frameworks governing these practices were neither designed for, nor have been systematically adapted to, the specific conditions of AI-mediated education (Future of Privacy Forum, 2024; Holmes et al., 2022).

The nature of this vacuum is not simply a lag in legislative drafting. It reflects a structural mismatch between the logic of general-purpose data protection frameworks, which are oriented toward individual transactions between consenting adults and identifiable data controllers, and the operational reality of AI education systems, in which students occupy a position of structural dependency, cannot meaningfully exit the data-collection relationship without foregoing access to education, and are frequently minors with constrained legal and practical capacity to exercise the rights that existing frameworks formally extend to them (Regan & Jesse, 2019). The Human Rights Watch investigation of EdTech deployment during the COVID-19 pandemic documented that approximately 89% (146 of 165) of EdTech products endorsed by governments in 49 countries appeared to engage in data practices that risked or infringed upon children's rights, including covert data harvesting, behavioural profiling, and transmission of data to advertising infrastructure (Han, 2022). This finding, drawn from a multi-jurisdictional review, underscores that the gap between deployment practice and regulatory protection is not hypothetical but has demonstrable empirical manifestations.

This article addresses three descriptive research questions, framed in terms of mapping and characterisation rather than normative assessment or institutional prescription: What categories of student data do AI education platforms deployed in Asia-Pacific collect, and what risks associated with those data categories have been documented in the existing literature? How comprehensively do the principal regulatory frameworks applicable in the Asia-

Pacific region — specifically the EU GDPR/AI Act, China's PIPL and algorithmic regulation, the ASEAN national PDPA series, the ASEAN Model Contractual Clauses (MCCs), and the US FERPA/COPPA framework — address AI-specific risks in educational settings? What structural dimensions of the regulatory gap between AI education deployment and student data protection can be systematically identified through a comparative mapping of these frameworks against documented deployment realities? These questions are descriptive in character. The article does not evaluate which regulatory framework is superior, does not propose how the identified gaps should be closed, and does not develop any institutional design. It provides, instead, the problem-diagnostic foundation on which subsequent normative and institutional analysis can be constructed.

The geographic scope of this article encompasses the Asia-Pacific region with primary focus on China and the principal ASEAN jurisdictions that have enacted personal data protection legislation: Singapore, Thailand, Indonesia, the Philippines, and Vietnam. The EU GDPR/AI Act and the US FERPA/COPPA framework are treated as comparative reference frameworks rather than as directly applicable law in the region, on the grounds that each has generated scholarship addressing the specific intersection of education and algorithmic systems, and each is directly relevant to the data protection obligations of platform providers operating globally (Regulation-AI.eu, 2026; sota.io, 2026; Papandrea, 2017).

The temporal scope is 2018 to June 2025, from the entry into force of the GDPR to the date of manuscript preparation. The AI system types examined include: intelligent tutoring systems (ITS) and adaptive learning platforms, AI-powered assessment and automated grading tools, learning analytics and student early-warning systems, and remote proctoring technologies. This typology is justified by the combination of high data collection intensity and significant impact on educational outcomes that characterises each category (IJRPR journal, 2025; EA Journals, 2025).

This article provides the empirical and descriptive foundation for a three-paper research series. It maps the regulatory gap without proposing solutions. The governance mechanisms through which that gap might be addressed, specifically, the failure of norm translation from legal principle to enforceable standard, are examined in the second article. The design of a recursive multi-layered legal architecture capable of closing those gaps systemically is the subject of the third article. This sequencing reflects a methodological commitment to separating problem diagnosis from normative prescription: the credibility of any proposed institutional response depends on the precision of the prior diagnosis.

## B. METHODS

This article adopts a systematic literature review (SLR) approach to identify and evaluate scholarship on artificial intelligence in education, student data governance, and the regulation of educational technologies. A systematic design was chosen to improve transparency and reduce selection bias, particularly given the interdisciplinary nature of the topic, which spans law, education, technology policy, and ethics. The review was informed by PRISMA-style principles of structured searching, screening, and eligibility assessment, adapted for a legal and socio-technical study rather than a quantitative meta-analysis.

The literature search was conducted in June 2025 across four major databases: Web of Science, Scopus, Google Scholar, and SSRN. These databases were selected to capture peer-reviewed academic research, legal scholarship, working papers, and policy-oriented literature. Because China forms an important jurisdictional focus in this article, a supplementary search was also conducted through CNKI to identify Chinese-language scholarship on AI deployment in education, student data protection, and the implementation of the Personal Information Protection Law (PIPL) and related regulatory measures.

The search strategy used a combination of Boolean keyword clusters linking three themes: artificial intelligence, education, and data governance. The core search string combined terms such as "AI," "artificial intelligence," "machine learning," and "algorithmic decision-making" with "education," "EdTech," "student," "school," and "learning analytics," together with governance-related terms including "data protection," "privacy," "surveillance," "regulation," "accountability," "bias," and "discrimination." These general searches were supplemented by jurisdiction-specific searches targeting legal frameworks and regulatory instruments, including the GDPR, the EU AI Act, PIPL, ASEAN data governance instruments, FERPA, and COPPA in educational contexts. For Chinese-language searches, equivalent terms were used, including 人工智能教育, 学生数据保护, and 个人信息保护.

Search results were screened in three stages. First, duplicate records retrieved across databases were removed. Second, titles and abstracts were reviewed to exclude clearly irrelevant materials. Third, full texts were assessed for eligibility. The inclusion criteria covered: (1) peer-reviewed articles, book chapters, and monographs published between January 2018 and June 2025; (2) policy documents, legislation, regulatory texts, and official guidance within the same period, as well as foundational legal instruments where necessary for context; (3) empirical studies documenting AI deployment in educational

settings; and (4) legal or policy analyses addressing data protection, governance, or regulatory accountability in education. The exclusion criteria covered purely technical studies without legal or governance relevance, non-institutional commentary lacking scholarly or policy value, and studies focused solely on non-AI digital education tools.

For each included source, key information was extracted concerning authorship, year, jurisdiction, type of AI application, legal or regulatory framework, and principal findings or arguments. Academic studies were also reviewed for methodological design, while legal and policy sources were assessed according to their authority, jurisdictional relevance, and practical significance. Institutional reports and grey literature were included only where they came from established bodies and provided identifiable evidentiary or analytical value.

The final review corpus comprised approximately 90 sources. These included peer-reviewed journal articles, books and book chapters, legislation and regulatory instruments, official guidance documents, institutional reports, selected court or enforcement materials, and a limited number of news sources used only as factual records for specific incidents or controversies. The corpus is weighted toward the European Union, China, and Singapore, reflecting both the maturity of their regulatory frameworks and the relative availability of scholarship. By contrast, literature on several Southeast Asian jurisdictions remains less developed, meaning that analysis in those contexts relies more heavily on primary legal texts and institutional materials.

This review has several limitations. It reflects the state of the literature as of June 2025, and therefore does not systematically include later developments. In addition, publication bias may favor studies documenting harms or controversies over routine or successful uses of AI in education. Nevertheless, the review provides a sufficiently broad and structured foundation for evaluating how existing legal and governance frameworks respond to the growing use of AI in educational environments.

The regulatory mapping section applies a descriptive comparative methodology. For each of the six frameworks, the analysis identifies: (a) the primary legal texts and their operative provisions relevant to educational AI; (b) any education-specific provisions or guidance; (c) the scope of coverage with respect to the AI system types identified; and (d) observable limitations in coverage as documented in the secondary literature. The analysis is explicitly non-evaluative.

The six frameworks analysed are below:

**Table 1.**

**Six Frameworks**

| Framework | Jurisdiction | Core Documents |
|---|---|---|
| GDPR + EU AI Act | European Union | Regulation (EU) 2016/679; Regulation (EU) 2024/1689 |
| PIPL + Algorithm Recommendation Provisions | China | PIPL (2021); Algorithm Recommendation Provisions (2022); Generative AI Interim Measures (2023) |
| National PDPA series | Singapore, Thailand, Philippines, Indonesia, Vietnam | PDPA 2012 (SG); PDPA 2019 (TH); DPA 2012 (PH); PDP Law 2022 (ID); Decree 13/2023 (VN) |
| ASEAN Model Contractual Clauses | ASEAN region | ASEAN MCCs (2021); ASEAN Data Management Framework (2021) |
| FERPA + COPPA | United States (reference) | 20 U.S.C. §1232g; 15 U.S.C. §6501 |
| UNESCO/OECD instruments | International | UNESCO AI in Education Recommendation (2021); OECD AI Principles (2019) |

This article does not evaluate which regulatory framework is superior to others, nor does it make prescriptive claims about how gaps should be addressed. Comparative observations are descriptive. The normative and institutional implications of the identified gaps are addressed in subsequent articles in this series. The literature review is limited to English- and Chinese-language sources; scholarship in Thai, Bahasa Indonesia, Filipino, and Vietnamese is not systematically included. The regulatory landscape in several jurisdictions continues to evolve, and some provisions discussed may have been supplemented by subsequent implementing regulations or guidance issued after the manuscript preparation date.

## C. RESULTS

### 1. AI in Education: Deployment Landscape in Asia-Pacific

a. Typology of AI Education Systems

AI educational systems vary substantially in the intensity of data collection they undertake and the degree to which their outputs influence consequential decisions about students. A functional taxonomy for the purposes of this analysis distinguishes four deployment types, ordered by increasing intensity on both dimensions.

**Type A: Intelligent Tutoring Systems and Adaptive Learning Platforms** represent the most widely deployed category (IJRPR, 2025; EA Journals, 2025). These systems collect continuous behavioural data during learning sessions, time-on-task, answer sequences, error patterns, click trajectories, and engagement metrics, and use that data to adjust content sequencing or recommendations in real time (ETH Zurich, 2025). Data collection intensity is high; decision impact is moderate in that the systems influence the learning pathway rather than directly determining outcomes.

**Type B: AI Assessment and Automated Grading Systems** collect structured response data (multiple-choice patterns, written text, code submissions) and apply machine-learning models to assign grades or scores (Eubanks, 2018; PubMed, 2025). Decision impact is high, since outputs directly affect academic records. The 2020 UK A-level examination controversy, in which an Ofqual-commissioned algorithm produced grades for approximately 280,000 students whose results were revised downward, systematically disadvantaging those from state schools relative to private school students, with 39.1% of teacher-assessed grades downgraded, represents the most extensively documented instance of consequential failure in this category (Failure Index, 2026; The Guardian, 2020a; BERA, 2021).

**Type C: Learning Analytics and Early Warning Systems** aggregate data across multiple sources, assignment submissions, platform interactions, library usage, attendance records, and sometimes social media, to generate risk scores or intervention triggers (Nature, 2025). Data collection intensity is highest in this category, and the outputs can affect teacher decisions, counselling referrals, and institutional resource allocation in ways that may not be transparent to affected students.

**Type D: Remote Proctoring Systems** operate during examination sessions and collect biometric data streams including facial video, eye-tracking patterns, keystroke dynamics, and acoustic monitoring (Scassa, 2022; University of Warwick, 2024). Under the EU AI Act Annex III, monitoring of prohibited behaviour during examinations is classified as a high-risk AI application (EU AI Act Annex III, 2024). Decision impact is direct and high: a flag generated by the system can result in examination cancellation or academic misconduct proceedings.

b. Deployment Scale in Asia-Pacific

The scale of AI education deployment in the Asia-Pacific region is substantial and growing rapidly, though systematic multi-jurisdiction data on

deployment rates remains limited in the peer-reviewed literature. China's AI education market is among the largest globally by deployment volume (TechWire Asia, 2026). The country has developed national plans to integrate AI into all stages of the education system, characterising the initiative as workforce infrastructure rather than curriculum enhancement (TechWire Asia, 2026). Adaptive learning platforms and intelligent tutoring systems have been deployed at scale in the K-12 sector, and the intersection of AI education with China's existing EdTech industry has produced a dense network of data processing relationships between schools, EdTech providers, and underlying cloud infrastructure.

Across ASEAN, government-led EdTech procurement accelerated significantly during and after the COVID-19 pandemic. Singapore has pursued targeted integration of AI literacy into primary school curricula and committed to AI teacher training across all levels (TechWire Asia, 2026). Indonesia, the Philippines, Thailand, and Vietnam have all experienced rapid growth in EdTech platform adoption, often driven by government emergency procurement decisions during school closures rather than deliberate pedagogical planning (Han, 2022). The COVID-19 pandemic constituted an accelerant of exceptional magnitude: the shift to remote education between 2020 and 2022 drove rapid adoption of AI proctoring systems, adaptive learning platforms, and learning management systems across the region, frequently in compressed procurement timescales that bypassed the evaluation processes institutions might otherwise have applied (Han, 2022). Human Rights Watch's 2022 investigation, encompassing 49 countries including numerous Asia-Pacific jurisdictions, found that approximately 89% of government-endorsed EdTech products appeared to engage in practices that risked or infringed upon children's data rights (Han, 2022).

c. Cross-Border Data Flow Dimensions

A distinctive feature of AI education deployment in Asia-Pacific is the prevalence of cross-border data flows inherent in the commercial architecture of EdTech markets. Educational institutions in the region have adopted commercial platforms developed and operated by companies headquartered outside the jurisdiction of the data subjects (Han, 2022; Gizmodo, 2022). Google Workspace for Education, Microsoft Education, and numerous US-headquartered EdTech SaaS platforms serve large student populations across Asia-Pacific, with data processed in server infrastructure located primarily in the United States, European Union, or Singapore (Han, 2022). Student data generated in a Thai primary school using a US-licensed adaptive learning platform will typically

traverse multiple jurisdictions before reaching its point of processing, subject along the way to the varying data protection regimes of each (Hogan Lovells, 2021; Lee et al., 2021).

A secondary pattern has emerged as Chinese EdTech companies have expanded into Southeast Asian markets, creating reverse data flows in which student data from ASEAN jurisdictions is processed under Chinese corporate governance structures (TechWire Asia, 2026). These flows remain under-examined in the scholarly literature but represent a structurally distinct accountability question from the more-studied flows toward US and European infrastructure.

## 2. Comparative Mirrors and Structural Reform Pathways

a. A Classification Framework for Student Data in AI Education Systems

The literature identifies a spectrum of data categories collected by AI education systems, distinguished by their content, their inferential potential, and the sensitivity implications of processing (Holmes et al., 2022; Regan & Jesse, 2019). The following taxonomy synthesises across multiple literature sources:

**Table 2.**

Taxonomy Synthesises Across Multiple Literature Sources

| Data Category | Specific Content | Sensitivity Dimension |
|---|---|---|
| Academic data | Grades, test scores, assignment submissions, learning progression records | Direct impact on admissions, employment, and future educational access |
| Behavioural data | Platform session duration, click and navigation patterns, interaction frequency, response latencies | Supports inference of cognitive states, engagement levels, and mental health indicators |
| Inferred/derived data | Learning style labels, risk scores, attention classifications, engagement ratings | Labelling and classification effects; self-fulfilling prophecy risks |
| Biometric data | Facial recognition, eye-tracking, keystroke dynamics, voice patterns | Highest sensitivity class; sensitive personal information under GDPR Art. 9 and PIPL Art. 28 |
| Metadata | IP addresses, device identifiers, geographic location, temporal access patterns | Re-identification potential through combination with other datasets |

The category of inferred or derived data warrants particular attention. AI education systems do not only process data that students knowingly provide;

they generate new data categories through inference, for example, classifying a student as "at risk" or assigning a learning style label that the student did not self-identify (PMC, 2024; Holmes, 2023). These inferred categories may not be recognised as personal data subject to protection under frameworks that do not explicitly extend their scope to algorithmic outputs, and students typically have no visibility into their existence or content (Holmes, 2023; Holmes et al., 2022).

b. Documented Risk Categories

The existing literature identifies several categories of risk associated with AI education data collection and processing that have been empirically documented rather than merely theorised (ScienceDirect, 2024; Nature, 2025; arXiv, 2024).

**Algorithmic bias and discriminatory impact.** The most extensively documented instance of algorithmic failure in educational assessment is the 2020 UK A-level grading system. The algorithm commissioned by Ofqual to generate grades during pandemic-related examination cancellations revised downward approximately 39.1% of teacher-assessed grades, affecting some 280,000 students (Failure Index, 2026; The Standard, 2020; The Guardian, 2020a). The downward adjustments were systematically skewed: students from state schools experienced larger negative adjustments than students from private institutions, and students from lower socioeconomic backgrounds were disproportionately affected (BERA, 2021; IEA, 2020). The controversy resulted in the resignation of the Ofqual chief executive, the reversal of the algorithm's outputs in favour of teacher assessments, and an ongoing debate about the accountability of public sector algorithmic decision-making (BBC, 2020a; BBC, 2020b). A separate and independent dimension of bias has been documented in remote proctoring systems. The US National Institute of Standards and Technology (NIST) published in 2019 a landmark study of 189 facial recognition algorithms across 99 developers, finding that for one-to-one matching, false-positive rates for Asian and African American faces ranged from a factor of 10 to 100 times higher compared to Caucasian faces (Grother et al., 2019). Multiple accounts in the proctoring literature have applied this documented pattern to argue that students from minority racial groups are disproportionately flagged during automated examination monitoring (Project Censored, 2021; Open Publishing, 2025). These documented cases establish that algorithmic bias in education is not a theoretical risk but an operational reality with measurable consequences.

**Commercial data re-use and secondary monetisation.** The 2022 Human Rights Watch investigation documented that approximately 89% (146 of 165) of government-endorsed EdTech products appeared to engage in data practices

that tracked children for behavioural profiling purposes, with many transmitting data to advertising technology infrastructure (Han, 2022). A civil complaint filed in December 2025 against Curriculum Associates (Case No. 1:25-cv-13942, D. Mass.) alleged practices involving the commercial monetisation of student reading assessment data collected via the widely-deployed i-Ready platform (Curriculum Associates Complaint, 2025; The Guardian, 2026). These cases represent documented instances of the commercial data re-use risk, occurring in contexts where existing regulatory frameworks did not provide effective prevention or redress.

**Cross-border transfer opacity.** Students and parents in Asia-Pacific jurisdictions using internationally-sourced EdTech platforms typically have no accessible information about where their data is processed, under what legal regime it is held, or what transfer mechanisms apply (Hogan Lovells, 2021; Gizmodo, 2022). Privacy policies in EdTech terms of service are frequently not translated into local languages, written at literacy levels inaccessible to the students they nominally apply to, and often do not specify the jurisdictions of data centre locations (TrustArc, 2015; Han, 2022). The combination of this opacity with the complexity of cross-border data protection obligations means that students and parents cannot practically exercise whatever rights their local framework nominally extends.

**Labelling, classification, and self-fulfilling prophecy effects.** Learning analytics early-warning systems assign risk classifications to students that influence teacher behaviour, counselling decisions, and institutional resource allocation (PMC, 2024; Regan & Jesse, 2019). The educational sociology literature has documented that such classifications can operate as self-fulfilling prophecies: students identified as "at risk" may receive differential attention, reduced academic expectations, or altered opportunity structures in ways that confirm the initial classification regardless of its accuracy (Regan & Jesse, 2019). Regan and Jesse (2019) identify the process by which personalised learning platforms engage in twenty-first-century student sorting and tracking as raising fundamental concerns about autonomy, non-discrimination, and the appropriate use of algorithmic inference in educational contexts.

**Structural vulnerability of minors.** A cross-cutting dimension of AI education data risk is the particular vulnerability of children and adolescents as data subjects. Minors lack the legal capacity to provide meaningful consent in most jurisdictions. Even where consent mechanisms are formally provided, the cognitive and informational requirements for understanding the implications of AI data processing in educational contexts exceed what can reasonably be

expected of children or adolescents (China Law Translate, 2022; XL Law Consulting, 2022). The institutional context of schooling adds a layer of structural coercion absent from general consumer data relationships: students who decline to use a school-mandated platform do not merely forgo a service; they risk exclusion from educational opportunities (Holmes et al., 2022; Holmes, 2023).

c. Data Flow Architecture

A descriptive account of AI education data flows in Asia-Pacific illustrates the multiplicity of data processing relationships involved in a typical deployment:

*Student → School learning management system or EdTech platform → Third-party AI model provider → Cloud infrastructure provider* (typically US, EU, or Singapore-based) → *Possible transmission to advertising technology stack* and/or *secondary use for model training* (Han, 2022; Gizmodo, 2022).

Each arrow in this chain represents a potential boundary of regulatory accountability. No single legal relationship encompasses the full lifecycle of the student's data, and — as elaborated in Section 6 — no existing regulatory framework provides a mechanism for cohering these relationships into a unified accountability structure.

## 3. Regulatory Frameworks: A Descriptive Mapping

a. The EU General Data Protection Regulation and AI Act

The GDPR represents the most comprehensive data protection framework currently in force globally, and its intersection with AI education systems is substantive. Several provisions are directly engaged by the deployment of AI systems in educational settings (Regulation-AI.eu, 2026; sota.io, 2026).

Article 5(1)(b) establishes purpose limitation as a core principle: personal data collected for one purpose may not be further processed in a manner incompatible with that purpose. Applied to AI education systems, this would in principle restrict the use of data collected for personalised learning to other commercial purposes such as advertising model training, the practice documented by Human Rights Watch (Han, 2022). Article 8 sets 16 as the default age of consent for digital services, with Member State discretion to lower this to 13, establishing that parental consent is presumptively required for data processing of children at the ages that constitute the primary school population (Eduface, 2026; sota.io, 2026b).

Article 22 provides data subjects with the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects. The application of this provision to AI educational assessment, including automated grading, learning pathway allocation, and early-warning risk classification, was directly at issue in the analysis of the UK A-level controversy, with the Information Commissioner's Office noting that GDPR's restrictions on solely automated decisions with legal effects were relevant to the Ofqual algorithm (ICO, 2021). Article 25 (data protection by design and by default) requires that data protection measures be integrated into system architecture from the outset, and Article 35 requires Data Protection Impact Assessments for processing likely to result in high risks to individuals.

The EU AI Act (Regulation (EU) 2024/1689, OJ L, 12 July 2024) classifies specific categories of AI educational application as high-risk under Annex III, Point 3 (EU AI Act Service Desk, 2024). High-risk designations cover: AI systems used to determine access or admission to educational institutions; systems used to evaluate learning outcomes; systems used to assess the appropriate level of education for an individual; and systems used to monitor and detect prohibited behaviour during examinations (EU AI Act Service Desk, 2024). Article 27 additionally requires deployers of high-risk AI systems to conduct Fundamental Rights Impact Assessments where the deployer is a body governed by public law or operates a critical infrastructure service (Eduface, 2026; Eduface, 2026b).

The GDPR/AI Act framework provides the most detailed global treatment of AI educational risks. Its direct applicability to Asia-Pacific jurisdictions is limited to the extraterritorial scope of Article 3 GDPR and the AI Act's extraterritorial provisions for AI system providers targeting EU markets. For the vast majority of students in Asia-Pacific whose data is not processed in connection with EU data subjects, GDPR/AI Act obligations bind only indirectly — primarily through the data export requirements of Articles 44-49 GDPR (Regulation-AI.eu, 2026; Eduface, 2026).

b. China's Regulatory Framework

China has, in the period from 2021 to 2023, developed a multi-instrument regulatory framework for personal information protection and algorithmic governance that is among the most comprehensive in Asia. The Personal Information Protection Law (PIPL), effective 1 November 2021, is the central instrument (Comparative AI, 2026). PIPL Article 28 defines "sensitive personal information" to include biometric data, minors' data (for those under 14), financial information, and health information; processing of sensitive personal

information requires separate consent and a personal information protection impact assessment (Comparative AI, 2026). Article 31 provides that the personal information of minors under 14 constitutes sensitive personal information, and that processing requires consent from a parent or guardian, with processors required to establish special rules for such processing (XL Law Consulting, 2022; China Law Translate, 2022).

PIPL Article 24 establishes rights with respect to automated decision-making, requiring that automated decisions be transparent and non-discriminatory, and granting individuals the right to request explanation of, and to refuse, decisions made solely by automated means that have significant impacts on their interests (Comparative AI, 2026). The 2022 Provisions on the Management of Algorithmic Recommendations in Internet Information Services require platforms using algorithmic recommendation to provide users with the option to turn off personalised recommendation (Article 17), operationalising PIPL Article 24 (Comparative AI, 2026).

China's three-pathway cross-border data transfer mechanism — security assessment by the Cyberspace Administration, personal information protection certification, and standard contractual clauses — provides a framework for the outbound transfer of personal data but applies general standards rather than education-specific requirements (Comparative AI, 2026). All major instruments: PIPL, the Data Security Law, the Algorithm Recommendation Provisions, and the Generative AI Measures, are designed as platform-neutral instruments. None contains sector-specific provisions for education (Comparative AI, 2026). PIPL Article 31's special protection for minors under 14 provides principle-level guidance but limited operational specificity for the diverse AI systems deployed in educational settings.

c. ASEAN National Frameworks

The ASEAN jurisdictions examined have each enacted personal data protection legislation, though at different points in time and with varying scope and enforcement capacity.

**Singapore's** Personal Data Protection Act 2012 (as amended in 2021) is the most mature in the region (PDPC, 2025). In March 2024, Singapore's Personal Data Protection Commission (PDPC) published Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment, which apply to any organisation whose products or services are "likely to be accessed by children," including technology-aided learning services (PDPC, 2024a; Bird & Bird, 2024). The guidelines address communication with children, consent

validity, reasonable purposes for processing, and data protection standards for children's data (Bird & Bird, 2024). These guidelines represent the only education-proximate guidance instrument in the ASEAN PDPA series; they are, however, non-binding (PDPC, 2024a).

**Thailand's** Personal Data Protection Act 2019 entered full enforcement in June 2022 (Future of Privacy Forum, 2024). **The Philippines'** Data Privacy Act 2012 applies general principles to educational data without sector-specific provisions. **Indonesia's** PDP Law 2022 entered into force in October 2022, with a two-year transition period (Library of Congress, 2022; One Asia Lawyers, 2023). **Vietnam's** Decree 13/2023 on Personal Data Protection entered into force on 1 July 2023 (EY Vietnam, 2023; LuatVietnam, 2023). Vietnam's Ministry of Education issued Official Dispatch 4567/BGDDT-CNTT in August 2024 directing educational institutions to strengthen compliance with Decree 13/2023, representing a rare instance of education-sector guidance cross-referencing the general data protection framework (Vietnam Ministry of Education, 2024).

**Table 3.**

ASEAN National Frameworks

| Jurisdiction | Primary Instrument | Effective Date | Education-Proximate Provisions | Children's Data |
|---|---|---|---|---|
| Singapore | PDPA 2012 (2021 rev.) | 2012 | Non-binding advisory guidelines (2024) | Yes (advisory) |
| Thailand | PDPA 2019 | Jun. 2022 | None | General provisions |
| Philippines | DPA 2012 | 2012 | None | General provisions |
| Indonesia | PDP Law 2022 | Oct. 2024 | None | Specific data category |
| Vietnam | Decree 13/2023 | Jul. 2023 | Ministry dispatch only (2024) | Sensitive category |

The ASEAN Model Contractual Clauses for Cross-Border Data Flows (MCCs), approved at the first ASEAN Digital Ministers' Meeting on 22 January 2021, provide a voluntary contractual framework for cross-border transfers of personal data within the ASEAN region (ASEAN, 2021; Mayer Brown, 2021). A joint guide issued by the EU and ASEAN in 2023 compared the MCCs with EU Standard Contractual Clauses (European Commission & ASEAN, 2023). The MCCs contain no education-specific provisions, and a text examination of the 2021 instrument confirms the absence of provisions specifically addressing

educational data categories or the particular position of students as data subjects (ASEAN, 2021; Hogan Lovells, 2021).

d. FERPA and COPPA as Reference Frameworks

FERPA, enacted in 1974 and codified at 20 U.S.C. §1232g, provides protections specific to educational records held by institutions receiving federal funding (US Department of Education, 2020). Under §99.31(a)(1), third-party service providers, including EdTech vendors, may be designated as "school officials" with legitimate educational interest, permitting access to student records, subject to requirements that they operate under school control and remain bound by FERPA obligations (US Department of Education, 2022; Public Interest Privacy Center, 2025). A 2013 review by the Fordham Center on Law and Information Policy found that fewer than 25% of the school-cloud service agreements examined specified the purpose for disclosure of student information, and no agreement specifically prohibited the sale and marketing of children's information (Reidenberg et al., 2013). The EdTech vendor, which may exercise the most significant practical control over student data, bears no direct statutory liability under FERPA (Public Interest Privacy Center, 2025; Tanuj Garg, 2026).

COPPA, codified at 15 U.S.C. §6501, applies specifically to operators of websites and online services directed at children under 13. It requires verifiable parental consent prior to data collection (FPF, 2016). A school consent exception allows educational institutions to act as agents of parents for consenting to EdTech data collection where the collection is for the school's educational benefit and for no commercial purpose, but courts and commentators have documented the practical difficulties of enforcing the scope limitation on commercial use (TrustArc, 2015; Tanuj Garg, 2026).

e. UNESCO and OECD International Instruments

UNESCO's Recommendation on the Ethics of Artificial Intelligence, adopted by acclamation by 193 Member States at UNESCO's General Conference on 23 November 2021, provides the most comprehensive international soft-law treatment of AI governance with relevance to education (UNESCO, 2021). The Recommendation addresses data protection, transparency, human oversight, and the importance of avoiding algorithmic bias. The OECD Recommendation of the Council on Artificial Intelligence, adopted at Ministerial level on 22 May 2019 (OECD Legal Instrument OECD/LEGAL/0449) and updated in 2024, articulates trustworthiness, transparency, accountability, and human-centredness as governance objectives (OECD, 2019). These instruments carry normative weight as expressions of international consensus but generate no binding obligations.

## 4. The Regulatory Gap: Four Structural Dimensions

The preceding sections establish that AI educational systems are deployed at scale across Asia-Pacific, that they collect sensitive student data and generate documented risks, and that the regulatory frameworks applicable in the region were not designed to address the specific conditions of those deployments. This section identifies and characterises four structural dimensions along which the gap between deployment reality and regulatory coverage is systematically observable.

a. Dimension One: The Context-Specificity Gap

**Description.** All major regulatory frameworks applicable to AI education in Asia-Pacific are designed as platform-neutral or sector-neutral instruments. They apply uniform standards to data processing regardless of whether the data subject is a child or an adult, whether exit from the data-collection relationship is practically available or not, and whether the processing occurs in a commercial marketplace or a compulsory educational institution. The distinctive structural features of the educational context, mandatory attendance, institutional power asymmetry, the developmental vulnerability of minors, and the absence of any market alternative to the assigned educational platform are not reflected in the rights architecture or compliance requirements of any of the national frameworks examined (Holmes et al., 2022; Holmes, 2023; Regan & Jesse, 2019).

The practical consequence is that AI education platforms and entertainment recommendation platforms are subject to equivalent regulatory treatment in most Asia-Pacific jurisdictions. The exit right that most frameworks treat as a partial substitute for substantive protection, the right to withdraw consent and cease use is illusory in a mandatory educational context (Regan & Jesse, 2019; Holmes et al., 2022).

Holmes et al. (2022) characterise this as one of the fundamental ethical challenges of AI in education: the educational context is one in which "students may have little choice but to engage with AI systems that collect extensive data about them," and in which the power imbalance between the institution and the student makes the framework of individual consent and opt-out structurally inadequate. The EU AI Act partially addresses this through its high-risk classification of specific AI educational applications under Annex III, a recognition that education requires category-specific regulatory attention. No equivalent sector-specific categorisation exists in the applicable ASEAN frameworks or in China's regulatory instruments (EU AI Act Service Desk, 2024; Regulation-AI.eu, 2026).

**Observable symptoms:** AI education platforms and social media platforms are subject to identical withdrawal consent requirements in most ASEAN jurisdictions; School procurement contracts for AI educational tools do not uniformly require education-specific data handling provisions; Impact assessment obligations (where they exist) do not require evaluation of educational equity risks or the structural vulnerability of student data subjects

b. Dimension Two: The Temporal Gap

**Description.** AI education systems are not static technological deployments; they are continuously updated systems in which the model, its training data, its output characteristics, and its functional scope can change substantially after initial deployment and compliance assessment (ScienceDirect, 2024; Nature, 2025). Regulatory compliance mechanisms in all frameworks examined are predominantly designed around a point-in-time assessment model: a data protection impact assessment is conducted prior to or at the point of deployment, privacy notices describe data processing at the time of drafting, and contractual arrangements specify data handling obligations at the time of contract execution.

The temporal mismatch between a dynamic AI system's ongoing evolution and the static nature of regulatory compliance documentation creates a gap that is particularly acute in educational settings where students may be subject to a platform's processing for multiple consecutive years. The Fordham Law School review (Reidenberg et al., 2013) found that fewer than 25% of school-cloud service agreements specified the purpose of disclosure, suggesting that the contractual framework for ongoing data management obligations is structurally weak even at baseline. PIPL's impact assessment requirement for sensitive personal information processing provides a basis for requiring ongoing review, but the practical implementation of that requirement in educational deployments has not been systematically documented (Comparative AI, 2026).

**Observable symptoms:** Platform service agreement updates do not uniformly require notification to educational institutions or re-engagement of consent mechanisms; Compliance documentation describes initial deployment conditions rather than the current operational state of AI systems; Audit obligations in existing frameworks typically focus on deployment-time rather than ongoing operational status

c. Dimension Three: The Cross-Border Accountability Gap

**Description.** When student data flows across national borders, as it routinely does in the Asia-Pacific EdTech market, data protection accountability

can be severed at jurisdictional boundaries (Hogan Lovells, 2021; Lee et al., 2021). The data subject's rights are governed by the law of their jurisdiction; the data importer's obligations are governed by the law of the importing jurisdiction; and the contractual or regulatory mechanisms designed to bridge these jurisdictions may not be accessible to, or enforceable by, the individual student.

The cross-border dimension of this gap manifests across three sub-dimensions. First, the data exporting jurisdiction may not have mechanisms that ensure its own data protection standards travel with the data: ASEAN MCCs are voluntary, non-binding on students, and may not incorporate the full set of rights available under the exporting jurisdiction's national law (ASEAN, 2021; Hogan Lovells, 2021). Second, the data importing jurisdiction may have lower or different standards. Third, and perhaps most practically significant, students and parents who believe their data rights have been violated have no accessible cross-border complaint mechanism: national supervisory authorities typically have jurisdiction only within their own territory, and cross-border cooperation mechanisms among ASEAN data protection authorities remain nascent (Future of Privacy Forum, 2024).

The ASEAN MCCs represent a regional attempt to address cross-border accountability, but their design prioritises commercial flexibility over data subject rights. The EU-ASEAN Joint Guide to MCCs and EU SCCs acknowledged significant structural differences between the two instruments in the transferee's obligations and in their enforcement architecture (European Commission & ASEAN, 2023). China's three-pathway cross-border transfer framework creates obligations primarily on the domestic data exporter rather than generating rights directly enforceable by data subjects (Comparative AI, 2026).

**Observable symptoms:** EdTech platform privacy policies typically do not disclose data centre locations or the jurisdictions under whose law processing occurs; Switching cloud infrastructure providers does not automatically trigger notification obligations to affected schools or students; Cross-border complaints by students or parents have no designated procedural pathway in any of the ASEAN frameworks examined

d. Dimension Four: The Multi-Actor Accountability Diffusion Gap

**Description.** AI education deployments typically involve a chain of actors whose respective contributions to data processing cannot easily be mapped onto the single "data controller" model that anchors liability in most data protection frameworks. A representative deployment chain might include: the EdTech platform developer; the platform operator; the school; the local education

authority; the cloud infrastructure provider; and, in some deployments, a separate AI model training service (Reidenberg et al., 2013; Public Interest Privacy Center, 2025; Han, 2022).

When the system produces harmful outputs- a biased grade, a false proctoring flag, an inaccurate risk classification- the question of who bears accountability for the resulting harm is genuinely unclear. The 2020 UK A-level controversy illustrated this accountability diffusion in practice: the resulting political controversy involved contested responsibility among the Department for Education, Ofqual, and the algorithm's developers, with initial positions taken by government figures attributing responsibility to the algorithm rather than to human decision-making (The Guardian, 2020b; BERA, 2021; IEA, 2020).

The GDPR addresses multi-actor situations through the concept of joint controllers (Article 26) and through the processor obligations in Articles 28-29. In Asia-Pacific frameworks, the joint controller concept is less developed: China's PIPL addresses joint processing through shared responsibility principles without the detailed GDPR structure; ASEAN PDPA instruments vary substantially in the depth of their treatment of processor obligations (Comparative AI, 2026; Future of Privacy Forum, 2024).

**Observable symptoms:** School procurement contracts commonly include provisions releasing EdTech vendors from liability for educational outcomes resulting from the platform's outputs; Post-incident accountability for AI-generated errors in educational assessment is distributed across multiple actors without clear primary liability; Students and parents who experience harm from AI education systems report difficulty identifying the appropriate complaint recipient (Scassa, 2022; The Guardian, 2024).

## 5. Stakeholder Tensions and Institutional Interest

a. Structural Tensions Among Key Stakeholders

The regulatory gaps identified in Section 6 do not persist in the absence of institutional actors with divergent interests. The following descriptive account identifies the primary stakeholder positions that give shape to the governance landscape, without assigning value judgments to any position.

**Table 4.**

Primary Stakeholder Positions

| Stakeholder | Primary Institutional Interest | Observable Tension with Student Data Protection |
|---|---|---|
| AI education platform developers and operators | Data accumulation for model refinement, market expansion, product differentiation through personalisation (Han, 2022; eLearning Industry, 2026) | Data minimisation and purpose limitation requirements constrain product iteration cycles |
| Educational institutions | Pedagogical improvement, administrative efficiency, cost management, procurement simplicity | Compliance assessment capacity is typically below what thorough vendor evaluation requires (Reidenberg et al., 2013; Holmes et al., 2022) |
| Students and parents | Educational quality, privacy protection, fair assessment, participation in consequential decisions (ETH Zurich, 2025) | Knowledge asymmetry about data practices; structural barriers to exercising withdrawal rights |
| Governments and regulatory authorities | Advancing digital education, maintaining data sovereignty, developing AI industries, protecting fundamental rights (TechWire Asia, 2026; Future of Privacy Forum, 2024) | Digital economy promotion objectives and student data protection obligations create genuine policy tensions |

b. Documented Instances of Institutional Friction

**Remote proctoring disputes.** Multiple universities across North America, Europe, and Asia-Pacific have experienced student protests, regulatory investigations, and in some cases litigation over remote proctoring systems that collect biometric data during examinations (Scassa, 2022; University of Warwick, 2024; The Guardian, 2024). The principal concerns documented in the literature include: the collection and retention of facial video and biometric data beyond examination periods; the disproportionate false-positive flagging of students from minority racial groups, a pattern supported by the NIST 2019 facial recognition study (Grother et al., 2019); and the absence of meaningful consent given the institutional requirement to use designated systems (Project Censored, 2021; Open Publishing, 2025). Scassa (2022) identifies a systematic failure of privacy impact assessment frameworks to adequately account for the compulsory character of educational data processing.

**Learning analytics early-warning system consequences.** The deployment of predictive analytics systems that assign risk scores to students based on learning management system engagement data has been documented as generating adverse outcomes for students who receive "at risk" designations (PMC, 2024; Regan & Jesse, 2019). Regan and Jesse (2019) identify these systems as a form of stratification that can encode existing socioeconomic inequalities into algorithmic outputs, potentially reinforcing rather than mitigating educational disadvantage.

**EdTech commercial data re-use.** The 2022 Human Rights Watch investigation documented the transmission of student data from government-endorsed EdTech platforms to advertising technology infrastructure, including in several Asia-Pacific jurisdictions (Han, 2022). The December 2025 civil complaint against Curriculum Associates (Case No. 1:25-cv-13942) alleged the use of student reading assessment data collected from school deployments for commercial purposes inconsistent with the educational use representations made to contracting schools (Curriculum Associates Complaint, 2025; The Guardian, 2026).

## D. DISCUSSION

### 1. Interactions Among the Four Gap Dimensions

The four structural dimensions of regulatory gap identified in Section 6 are not independent; they interact and reinforce one another in ways that compound their individual effects. The context-specificity gap (Dimension One) means that even well-designed general data protection frameworks do not engage the particular vulnerabilities of student data subjects. The temporal gap (Dimension Two) means that even the regulatory provisions that do engage those vulnerabilities may become outdated quickly as AI systems evolve. The cross-border accountability gap (Dimension Three) means that even current and applicable obligations may not attach to the entities that process student data in the most consequential ways. And the multi-actor accountability diffusion (Dimension Four) means that even when obligations do attach, the entity bearing the obligation may have limited practical influence over the processing — and students may be unable to identify where to seek redress.

The cumulative consequence of these four dimensions operating simultaneously is that AI education platforms can, as a matter of observed practice, collect extensive student data with low friction, use it in ways that were not disclosed at collection, transfer it across jurisdictions without those jurisdictions' data protection requirements accompanying it, and distribute accountability for any resulting harm across a chain of actors in a way that makes enforcement prohibitively complex. This is not a claim that all AI education platforms engage in harmful practices; it is a characterisation of the structural conditions under which harmful practices can occur without effective regulatory response.

### 2. Limitations of This Analysis

The descriptive scope of this article entails several acknowledged limitations. The literature review reflects the composition of the accessible scholarly record, which underrepresents Asian-language scholarship and may not fully capture regulatory developments in jurisdictions with less developed English-language commentary. The regulatory frameworks assessed were current as of June 2025; subsequent legislative or guidance developments may have addressed some of the gaps described. The comparative analysis is institutional rather than empirical: it does not report on actual compliance rates, enforcement actions, or observed regulatory practices across the jurisdictions, which would require a different methodology. Finally, the characterisation of the four gap dimensions is a constructed analytical taxonomy derived from synthesis of the literature; alternative taxonomies are possible and may yield different insights.

### 3. Directions for Subsequent Research

This article has mapped four structural dimensions of the regulatory gap between AI education deployment and student data protection in Asia-Pacific jurisdictions. The characterisation of these gaps as structural raises the question of why existing frameworks, which contain principles relevant to the identified problems, fail to translate those principles into effective regulatory outcomes. That question — specifically, why the norm translation process from legal principle to enforceable standard breaks down in the context of AI education governance — is the subject of the second article in this series. The design question — what legal architecture could systematically address these gaps — is addressed in the third article.

## E. CONCLUSION

This article has identified and described four structural dimensions of the regulatory gap between AI educational system deployment and student data protection in Asia-Pacific jurisdictions, on the basis of a systematic literature review and a descriptive comparative analysis of six regulatory frameworks.

First, existing frameworks are platform-neutral by design, and that design renders them structurally unable to engage the specific vulnerabilities of students in AI-mediated educational environments. Students' effective inability to exit

mandated data-collection relationships, their developmental stage as minors, and the institutional power asymmetry of compulsory education are not accommodated by frameworks built around individual consent and exit rights (Holmes et al., 2022; Regan & Jesse, 2019).

Second, the static compliance model- assessment at deployment, documentation at a point in time cannot track the continuous evolution of AI systems, creating a growing divergence between what regulatory documentation says about a system and what that system actually does (Reidenberg et al., 2013; Comparative AI, 2026).

Third, cross-border data flows, which are intrinsic to the commercial architecture of Asia-Pacific EdTech markets, fragment accountability at jurisdictional boundaries in ways that no existing regional instrument adequately addresses. The ASEAN MCCs provide a voluntary contractual mechanism but neither bind data subjects' rights in the receiving jurisdiction nor create an accessible complaint mechanism for affected students (ASEAN, 2021; Hogan Lovells, 2021).

Fourth, the multi-actor chain typical of AI education deployments disperses accountability in ways that cannot be resolved by frameworks oriented around a single identifiable data controller. When harm occurs, the distribution of responsibility across developers, operators, institutions, authorities, and infrastructure providers makes identifying an accountable party, and exercising a right against it, a practical challenge beyond the capacity of most affected students and families (Reidenberg et al., 2013; Holmes et al., 2022).

These four dimensions are mutually reinforcing: each amplifies the effect of the others. Their concurrent operation means that incremental reform, adding an education-specific provision to a general PDPA, or extending an impact assessment requirement to AI systems, may address individual symptoms without altering the structural conditions that generate them. Whether, and how, those structural conditions can be altered is the question that the subsequent articles in this series are designed to address.

## REFERENCES:

### Legislation and Official Regulatory Instruments

ASEAN. (2021a). ASEAN Model Contractual Clauses for Cross-Border Data Flows. ASEAN Secretariat. https://asean.org/wp-content/uploads/3-

ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

ASEAN. (2021b). ASEAN Data Management Framework and Model Contractual Clauses on Cross-Border Data Flows: Implementing Guidelines. ASEAN Secretariat. https://asean.org/wp-content/uploads/2021/08/Implementing-Guidelines-for-ASEAN-Data-Management-Framework-and-Cross-Border-Data-Flows-Mechanism.pdf

China. (2021a). Personal Information Protection Law of the People's Republic of China [个人信息保护法] (Adopted August 20, 2021, effective November 1, 2021). National People's Congress. https://www.chinalawtranslate.com/en/personal-information-protection-law/

China. (2021b). Data Security Law of the People's Republic of China [数据安全法] (Effective September 1, 2021). National People's Congress. https://www.chinalawtranslate.com/en/data-security-law/

China. (2022). Provisions on the Management of Algorithmic Recommendations in Internet Information Services [互联网信息服务算法推荐管理规定] (Effective March 1, 2022). Cyberspace Administration of China. https://www.chinalawtranslate.com/en/algorithms/

China. (2023). Interim Measures for the Management of Generative Artificial Intelligence Services [生成式人工智能服务管理暂行办法] (Effective August 15, 2023). Cyberspace Administration of China. https://www.chinalawtranslate.com/en/2023-generative-ai-interim/

European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

European Parliament and Council. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, 1–144. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Personal Data Protection Law] (Enacted October 17, 2022). https://www.loc.gov/item/global-legal-monitor/2022-12-18/indonesia-personal-data-protection-act-enters-into-force

Philippines. (2012). Republic Act No. 10173 — Data Privacy Act of 2012 (Signed August 15, 2012). National Privacy Commission. https://www.privacy.gov.ph/data-privacy-act/

Singapore. (2012, amended 2021). Personal Data Protection Act 2012 (Cap. 26F). Personal Data Protection Commission. https://www.pdpc.gov.sg/overview-of-pdpa/the-personal-data-protection-act

Thailand. (2019). Personal Data Protection Act B.E. 2562 (2019; full enforcement June 2022). Personal Data Protection Committee. https://www.pdpc.or.th/en/

United States. (1974). Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 C.F.R. Part 99. https://studentprivacy.ed.gov/ferpa

United States. (1998). Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506; 16 C.F.R. Part 312. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Vietnam. (2023). Decree No. 13/2023/ND-CP of 17 April 2023 on Personal Data Protection (Effective July 1, 2023). Government of Vietnam. https://lawnet.vn/thong-tin-phap-luat/en/van-ban-phap-luat/decree-no-13-2023-nd-cp-dated-april-17-2023-personal-data-protection-88048.html

**International and Intergovernmental Documents**

European Commission & ASEAN. (2023). Joint Guide to the ASEAN Model Contractual Clauses and the EU Standard Contractual Clauses. European Commission. https://commission.europa.eu/system/files/2023-05/Final%20Joint_Guide_to_ASEAN_MCC_and_EU_SCC.pdf

OECD. (2019). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). OECD. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence (SHS/BIO/REC-AIETHICS/2021). UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000380455

**Official Guidance Documents**

Information Commissioner's Office. (2021). Decision Notice IC-70514-H7K5. UK Information Commissioner's Office. https://ico.org.uk/action-weve-taken/decision-notices/2021/08/ic-70514-h7k5/

Personal Data Protection Commission. (2024a). Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment (Published March 28, 2024). PDPC Singapore. https://www.pdpc.gov.sg/guidelines-and-consultation/2024/03/advisory-guidelines-on-the-pdpa-for-childrens-personal-data-in-the-digital-environment

Personal Data Protection Commission. (2024b). Advisory Guidelines for the Education Sector (Revised April 2024). PDPC Singapore. https://www.pdpc.gov.sg/guidelines-and-consultation/2018/09/advisory-guidelines-for-the-education-sector

U.S. Department of Education. (2020). Protecting student privacy: Education technology vendors. Student Privacy Policy Office. https://studentprivacy.ed.gov/audience/education-technology-vendors

U.S. Department of Education. (2022). Responsibilities of third-party service providers under FERPA (FAQ). Student Privacy Policy Office. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Vendor%20FAQ.pdf

Vietnam Ministry of Education and Training. (2024, August 22). Official Dispatch 4567/BGDDT-CNTT on strengthening personal data protection and network information security. https://lawnet.vn/thong-tin-phap-luat/en/thong-bao-van-ban-moi/enhancement-of-personal-data-protection-and-cyber-information-security-in-education-and-training-sector-official-dispatch-no-4567-bgddt-cntt-dated-august-22-2024.html

**Court Documents**

M.C. v. Curriculum Associates, Inc., No. 1:25-cv-13942-FDS (D. Mass. filed Dec. 22, 2025). https://edtech.law/wp-content/uploads/2026/04/Curriculum-Assoc-Complaint.pdf

**Journal Articles and Books**

Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) Part 3: Demographic effects (NISTIR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Holmes, W. (2023). The unintended consequences of artificial intelligence and education. UCL Discovery. https://discovery.ucl.ac.uk/id/eprint/10179267/

Holmes, W., & Porayska-Pomsta, K. (Eds.). (2022). The ethics of artificial intelligence in education: Practices, challenges, and debates (1st ed.). Routledge. https://doi.org/10.4324/9780429329067

Holmes, W., Porayska-Pomsta, K., Holstein, K., Sutherland, E., Baker, T., Shum, S. B., Santos, O. C., Rodrigo, M. T., Cukurova, M., Bittencourt, I. I., & Koedinger, K. R. (2022). Ethics of AI in education: Towards a community-wide framework. International Journal of Artificial Intelligence in Education, 32(3), 504–526. https://doi.org/10.1007/s40593-021-00239-1

Porayska-Pomsta, K., Holmes, W., & Nemorin, S. (2024). The ethics of AI in education. arXiv. https://arxiv.org/abs/2406.11842

Regan, P. M., & Jesse, J. (2019). Ethical challenges of edtech, big data and personalized learning: Twenty-first-century student sorting and tracking. Ethics and Information Technology, 21(3), 167–179. https://doi.org/10.1007/s10676-018-9492-2

Reidenberg, J., Russell, N. C., Kovnot, J., Norton, T. B., Cloutier, R., & Alvarado, D. (2013). Privacy and cloud computing in public schools. Fordham Center on Law and Information Policy. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1001&context=clip

Scassa, T. (2022). The surveillant university: Remote proctoring, AI, and human rights. Canadian Journal of Comparative and Contemporary Law, 8, 271–312. https://www.cjccl.ca/wp-content/uploads/2022/10-Scassa.pdf

Selwyn, N. (2019). Should robots replace teachers? AI and the future of education. Polity Press.

**Reports and Investigative Documents**

Future of Privacy Forum. (2016). COPPA and FERPA compliance for companies in the EdTech industry. https://fpf.org/wp-content/uploads/2016/03/COPPA-and-FERPA-Compliance-for-Companies-in-the-EdTech-Industry.pdf

Future of Privacy Forum. (2024). Regulatory strategies of data protection authorities in the Asia-Pacific Region: 2024 and beyond (FPF Issue Brief). https://fpf.org/wp-content/uploads/2024/09/FPF-Issue-Brief-APAC-DPA-Strategies-2024-1.pdf

Han, H. J. (2022). "How dare they peep into my private life?": Children's rights violations by governments that endorsed online learning during the

COVID-19 pandemic. Human Rights Watch. https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

Public Interest Privacy Center. (2025). Fixing FERPA: Enhancing EdTech accountability. https://publicinterestprivacy.org/edtech-data-sharing/

**News and Web Sources Cited as Factual Record**

BBC News. (2020a, August 19). A-levels: Ofqual's 'cheating' algorithm under review. BBC. https://www.bbc.com/news/technology-53836453

BBC News. (2020b, August 18). A-levels: Algorithm at centre of grading crisis 'unlawful' says Labour. BBC. https://www.bbc.com/news/uk-politics-53837722

BERA. (2021, May 20). The great algorithm fiasco. British Educational Research Association. https://www.bera.ac.uk/blog/the-great-algorithm-fiasco

Bird & Bird. (2024, April 1). Singapore's PDPC issues advisory guidelines on the PDPA for children's personal data in the digital environment. Bird & Bird. https://www.twobirds.com/en/insights/2024/singapore/singapore-pdpc-issues-advisory-guidelines-on-the-pdpa

Evening Standard. (2020, August 12). A Level results day 2020 in numbers: Key stats. Evening Standard. https://www.standard.co.uk/news/education/a-level-results-day-pass-rate-downgraded-a4523661.html

Failure Index. (2026, June 3). Ofqual's grading algorithm downgraded 39% of A-level results before being reversed in days. Failure Index. https://failureindex.ai/failures/ofqual-grading-algorithm-downgraded-39-level

Gizmodo. (2022, May 24). Remote learning software tracked kids' data to sell to advertisers and brokers: Report. Gizmodo. https://gizmodo.com/remote-learning-data-brokers-privacy-1848975202

Hogan Lovells. (2021, May 10). Aspiring for harmonization: ASEAN's model clauses for data transfers. Hogan Lovells. https://www.hoganlovells.com/en/publications/aspiring-for-harmonization-aseans-model-clauses-for-data-transfers

IEA. (2020, September 22). Lessons from the UK's A-Level algorithm debacle. Institute of Economic Affairs. https://iea.org.uk/lessons-from-the-uks-a-level-algorithm-debacle/

Library of Congress. (2022, December 17). Indonesia: Personal Data Protection Act enters into force. Global Legal Monitor. https://www.loc.gov/item/global-legal-monitor/2022-12-18/indonesia-personal-data-protection-act-enters-into-force

Mayer Brown. (2021, February 7). Finding harmony — ASEAN Model Contractual Clauses and Data Management Framework launched. Mayer Brown. https://www.mayerbrown.com/en/insights/publications/2021/02/finding-harmony-asean-model-contractual-clauses-and-data-management-framework-launched

Project Censored. (2021, November). Algorithmic bias in online test-monitoring programs. Project Censored. https://www.projectcensored.org/algorithmic-bias-in-online-test-monitoring-programs/

TechWire Asia. (2026, April 12). Mandatory AI literacy: China joins the UAE and India. Where is Southeast Asia? TechWire Asia. https://techwireasia.com/2026/04/ai-literacy-national-education-workforce/

The Guardian. (2020a, August 14). 'Punishment by statistics': The father who foresaw A-level algorithm flaws. The Guardian. https://www.theguardian.com/education/2020/aug/14/punishment-by-statistics-the-father-who-foresaw-a-level-algorithm-flaws

The Guardian. (2020b, August 17). A-level and GCSE results in England to be based on teacher assessments in U-turn. The Guardian. https://www.theguardian.com/education/2020/aug/17/a-levels-gcse-results-england-based-teacher-assessments-government-u-turn

The Guardian. (2024, April 18). Are your kids being spied on? The rise of anti-cheating software in US schools. The Guardian. https://www.theguardian.com/education/2024/apr/18/us-schools-anti-cheating-software-proctorio

The Guardian. (2026, June 11). California parents sue i-Ready maker over student data collection. The Guardian. https://www.theguardian.com/us-news/2026/jun/11/california-parents-sue-i-ready-student-data