

Children's Privacy and Digital Education in Indonesia: Regulating the Collection of Student Data by Schools and Educational Platforms

Sulaiman Sulaiman*^{ID}

Universitas Negeri Jakarta, Jakarta, Indonesia
sulaiman@students.unj.ac.id

DOI: <https://doi.org/10.65815/9bpbb826>

Submitted: 18-12-2025

Revised: 22-03-2026, 05-04-2026

Accepted: 10-04-2026

*Corresponding Author

Abstract

The rapid adoption of digital learning platforms in Indonesian schools has increased the collection and processing of children's personal data. Student information may include identity data, educational performance, behavioral records, and digital activity. Because children are particularly vulnerable to privacy risks, the expansion of educational technology raises important human rights concerns. This article examines the protection of children's privacy in Indonesia's digital education ecosystem. Using normative juridical research and policy analysis, the study evaluates personal data protection, education regulation, school responsibilities, and digital platform governance. The article argues that educational necessity should not become a blanket justification for unlimited collection or retention of children's personal information. Schools and technology providers should apply data minimization, purpose limitation, security safeguards, parental or appropriate consent mechanisms, and age-sensitive privacy protections. The study proposes a child-rights-based governance framework requiring clear contractual arrangements between schools and technology providers, transparent privacy notices, independent oversight, and accessible remedies. The article concludes that digital education policy should integrate children's best interests and privacy rights into technology procurement and educational governance.

[Adopsi pesat platform pembelajaran digital di sekolah-sekolah Indonesia telah meningkatkan pengumpulan dan pengolahan data pribadi anak. Informasi siswa dapat mencakup data identitas, prestasi pendidikan, catatan perilaku, dan aktivitas digital. Karena anak-anak sangat rentan terhadap risiko privasi, perluasan teknologi pendidikan menimbulkan kekhawatiran penting terkait hak asasi manusia. Artikel ini mengkaji perlindungan privasi anak dalam ekosistem pendidikan digital Indonesia. Dengan menggunakan riset yuridis normatif dan analisis kebijakan, studi ini mengevaluasi perlindungan data pribadi, regulasi pendidikan, tanggung jawab sekolah, dan tata kelola

platform digital. Artikel ini berpendapat bahwa kebutuhan pendidikan tidak boleh menjadi pembenaran umum untuk pengumpulan atau penyimpanan informasi pribadi anak tanpa batas. Sekolah dan penyedia teknologi harus menerapkan minimalisasi data, pembatasan tujuan, pengamanan, mekanisme persetujuan orang tua atau yang sesuai, dan perlindungan privasi yang peka terhadap usia. Studi ini mengusulkan kerangka kerja tata kelola berbasis hak anak yang membutuhkan pengaturan kontraktual yang jelas antara sekolah dan penyedia teknologi, pemberitahuan privasi yang transparan, pengawasan independen, dan solusi yang mudah diakses. Artikel ini menyimpulkan bahwa kebijakan pendidikan digital harus mengintegrasikan kepentingan terbaik anak dan hak privasi ke dalam pengadaan teknologi dan tata kelola pendidikan.]

Keywords: Children's rights, privacy, digital education, student data, Indonesia

Introduction

Digital technology has become increasingly embedded in educational systems, changing how schools teach, assess, communicate, administer student records, and evaluate educational performance. Learning management systems, cloud-based applications, online examinations, attendance platforms, student information systems, artificial intelligence, and learning analytics can generate information at a scale that was difficult to imagine in conventional classrooms. The data may include names, identification numbers, contact details, academic grades, attendance records, behavioral observations, disability-related information, communications, device information, and detailed records of interaction with digital learning environments. The expansion of these systems offers substantial educational benefits, but it also changes the relationship between children and institutions because routine educational participation increasingly generates persistent digital records. Research on e-learning has shown that educational software commonly gathers personal information and metadata and that such information is increasingly processed by third-party providers outside the direct institutional environment (Alier et al. 2021).

The privacy implications become more serious when the data subjects are children. Children are not simply smaller versions of adult data subjects. Their capacity to understand complex data-processing practices, negotiate contractual terms, assess long-term consequences, and exercise meaningful control over personal information develops progressively. The United Nations Committee on the Rights of the Child has recognized that digital technologies affect a broad range of children's rights and has specifically emphasized the need to protect children's privacy in the digital environment (Committee on the Rights of the Child 2021).

Privacy in this context should therefore be understood not merely as secrecy but as a condition supporting dignity, autonomy, identity, freedom of expression, and protection against exploitation. The increasing use of data-driven education consequently creates a tension between the legitimate institutional need to manage education and the child's right not to become the object of unrestricted digital observation.

Indonesia has developed a more substantial legal basis for addressing these concerns through Law No. 27 of 2022 concerning Personal Data Protection. The law recognizes children's personal data as requiring special treatment and requires parental or guardian consent for processing children's personal data. This development is significant because it moves beyond a general understanding of privacy and establishes a specific legal obligation concerning children. Indonesian scholarship has nevertheless identified continuing challenges concerning the practical formulation and implementation of children's privacy protection, particularly because detailed mechanisms concerning consent, institutional responsibilities, and digital-platform governance require further operationalization (Novanta and Pratami 2022). The emergence of digital education makes this regulatory question especially important because schools frequently function simultaneously as educational institutions, data controllers, and gateways through which children are required to access third-party technological services.

The central argument of this article is that the educational character of data processing should not automatically make such processing legitimate without substantive limits. Schools undoubtedly need certain student information to deliver education, maintain records, administer examinations, protect students, and comply with legal obligations. However, the existence of a legitimate educational purpose does not necessarily justify collecting every technically available data point. Learning analytics research demonstrates that educational technologies can progressively expand the amount and granularity of information collected about students, while institutional policies may struggle to keep pace with technological capabilities (Prinsloo, Slade, and Khalil 2022). The appropriate legal question is therefore not whether schools may collect student data, but which data are genuinely necessary, for what purpose, for how long, by whom, under what safeguards, and with what remedies when the system fails.

This article employs normative juridical research combined with policy analysis and interdisciplinary review of peer-reviewed scholarship on children's privacy, educational technology, data governance, learning analytics, and digital rights. The normative component examines Indonesian constitutional principles, Law No. 27 of 2022 concerning Personal Data Protection, child protection legislation, electronic-system governance, and relevant educational regulation. International standards are used as interpretive references, particularly the Convention on the Rights of the Child and General Comment No. 25 on children's rights in relation to the digital environment. The analysis focuses on the principles

of the best interests of the child, privacy, data minimization, purpose limitation, security, transparency, participation, accountability, and effective remedy.

The literature analysis draws on peer-reviewed journal articles published no later than 2025. Particular attention is given to studies examining student privacy, learning analytics, school datafication, commercial EdTech, data governance, informed consent, cybersecurity, and children's digital rights. The study is analytical rather than empirical: it does not claim to measure the practices of a particular Indonesian school or educational platform. Instead, it identifies legal and governance problems that emerge from the interaction between Indonesian regulation and the technological characteristics of contemporary digital education. The comparative literature is used cautiously, not to transplant foreign legal regimes directly into Indonesia, but to identify governance principles capable of strengthening the domestic framework.

Digital Education and the Expansion of Children's Datafication

The transformation of education into a data-intensive environment has altered the nature of student records. Traditional school records generally consisted of relatively stable information such as enrollment data, grades, attendance, and disciplinary records. Digital education can generate substantially more granular information, including login frequency, time spent on particular learning materials, clicks, search behavior, assignment histories, interaction patterns, device information, and inferred indicators of engagement or performance. Datafication therefore changes not only the quantity of information available to schools but also what institutions can infer about students. Decuyper (2021) explains that educational data practices involve interconnected infrastructures, processes of datafication, and individual data points that acquire meaning through institutional practices. This means that privacy risks cannot be understood solely by examining individual pieces of information; the combination and interpretation of apparently ordinary data can create detailed profiles of children's educational behavior.

Learning analytics illustrates this transformation particularly clearly. Educational institutions increasingly use student data to identify students who may require additional support, predict academic outcomes, personalize learning, and improve institutional decision-making. These objectives can produce legitimate educational benefits. However, the same systems may generate concerns about surveillance, classification, automated decision-making, and the secondary use of data. Research has shown that students' privacy concerns are influenced by perceptions of privacy risk and the degree of control they believe they have over their information (Mutimukwe et al. 2022). Although much of this research concerns higher education, the underlying concern is arguably stronger for children because younger students generally possess less capacity to negotiate data practices and may have little realistic ability to refuse technologies mandated by schools.

The problem is particularly acute where educational technologies are supplied by private companies. Schools may adopt commercial platforms because they offer sophisticated learning management, communication, analytics, or assessment capabilities at relatively low institutional cost. Yet outsourcing technological infrastructure can create a complex chain of data processing involving schools, platform providers, cloud-service companies, analytics vendors, and other third parties. Alier et al. (2021) argue that student information is increasingly stored and processed outside the direct control of educational institutions, creating risks associated with unauthorized access, disclosure, and secondary use. A recent socio-legal analysis of EdTech governance similarly found that schools may possess limited expertise and resources to scrutinize how commercial providers process children's information (Williamson et al. 2023). The institutional outsourcing of data processing therefore cannot mean the outsourcing of legal and ethical responsibility.

Datafication also changes the educational experience itself. When students know that their behavior is continuously recorded, measured, and potentially evaluated, the classroom can become a site of surveillance rather than merely a space for learning. Pangrazio, Selwyn, and Cumbo's research into school datafication found that students experienced data practices through power, surveillance, accountability, and a limited sense of agency. This is particularly relevant where digital monitoring extends beyond academic achievement into behavioral or emotional assessment. Multimodal learning analytics can involve cameras, sensors, wearables, and other technologies capable of capturing increasingly intimate information about students. Prinsloo, Slade, and Khalil (2023) warn that such practices raise serious concerns when data collection becomes intrusive without sufficiently clear educational justification.

The expansion of datafication therefore requires a distinction between educational usefulness and legal necessity. The fact that data could potentially improve educational predictions does not establish that the data must be collected. This distinction is central to data minimization. If a school can accomplish a legitimate educational purpose using less intrusive information, collecting additional information may become difficult to justify. The principle is particularly important for children because data collected during childhood can remain available long after the original educational purpose has ended. A child's behavioral profile, academic history, learning difficulties, or inferred characteristics may become part of a persistent digital identity. Privacy protection must consequently address the entire data lifecycle rather than focusing only on the moment when information is initially collected.

Children's Privacy, Consent, and the Limits of Educational Necessity

The principle of consent occupies an important position in data protection law, but children's educational environments demonstrate why consent cannot be treated

as the sole safeguard. Indonesian Law No. 27 of 2022 requires specific treatment of children's personal data and parental or guardian consent for its processing. This establishes an important procedural protection, yet consent alone cannot resolve the structural imbalance between schools, technology providers, parents, and children. A school may make a particular digital platform effectively necessary for participation in education. In such circumstances, a parent who technically agrees to data processing may have little meaningful alternative if refusing the platform would interfere with the child's ability to participate in ordinary educational activities. Consent can therefore become formal rather than genuinely voluntary.

This concern is consistent with broader scholarship on educational data. Jones (2019) argues that informed consent is important for promoting student privacy and autonomy but also recognizes that Big Data environments make traditional consent mechanisms difficult to sustain. Students may not understand the full extent of data flows or the future uses of information at the time consent is obtained. Research involving university students similarly found that students often lack awareness of learning analytics practices and express strong preferences for transparency concerning what information is collected, why it is collected, and who can access it (Jones et al. 2020). For children, the problem is even more pronounced because privacy notices and consent forms may be written for adults, using legal and technical language that is difficult for young users to understand.

A rights-based approach should consequently distinguish parental authorization from the child's own participation. Parents or guardians have an important legal role in protecting children's interests, but children should not be treated as passive objects of decisions concerning their digital identities. The Convention on the Rights of the Child recognizes the child's evolving capacities and the importance of participation in matters affecting them. General Comment No. 25 reinforces the relevance of children's views in the digital environment. Privacy governance in schools should therefore incorporate age-appropriate explanations and opportunities for children to understand how their information is used. This does not mean requiring young children to provide legally decisive consent in every situation. Rather, it means recognizing that respect for children's developing autonomy should form part of the design of digital education systems.

The limits of consent become clearer when data are processed for purposes beyond immediate educational delivery. A school may legitimately need a student's name, enrollment information, attendance record, and assessment results. It does not follow that the same data may automatically be used for commercial profiling, targeted advertising, unrelated product development, or indefinite algorithmic experimentation. Research on educational data privacy has repeatedly identified the tension between legitimate educational interests and secondary commercial or institutional purposes (Hillman 2022; Rivera-Vargas, Raffaghelli, and Mico-Puigcercys 2024). Where a platform operates according to a commercial business model, schools must be especially careful to ensure that children's educational

participation does not become a mechanism for generating commercial value from their personal information.

Data minimization and purpose limitation are therefore more fundamental than consent alone. If processing is excessive, a signed consent form should not automatically legitimize it. Similarly, an educational purpose stated in broad language should not authorize indefinite reuse of student information. The purposes of processing should be specific, understandable, and demonstrably connected to educational functions. Research on educational data privacy has emphasized that privacy cannot be reduced to technical controls because institutional governance, accountability, and the social meaning of data are equally important (Prinsloo, Slade, and Khalil 2022).

The question of consent also becomes complicated where schools use automated profiling or artificial intelligence. Predictive systems may infer that a student is at risk of dropping out, has low engagement, is likely to experience learning difficulties, or belongs to a particular behavioral category. Such inferences can affect how teachers and institutions treat students even when the underlying prediction is probabilistic. The use of algorithmic profiling raises concerns about transparency, contestability, and discrimination. A student may know what information they directly supplied but have no knowledge of the inferences generated from that information. Children's privacy protection should therefore extend beyond raw data to derived profiles and algorithmic conclusions that materially affect educational opportunities.

Responsibilities of Schools and Educational Technology Providers

Schools occupy a central position in the governance of children's educational data because they determine whether and how digital systems are integrated into compulsory or highly consequential educational activities. Their responsibility should not end when a technology provider is selected. A school that contracts with a third-party platform remains responsible for ensuring that the processing arrangement is consistent with legal requirements and the best interests of students. Research on school data practices demonstrates that educational institutions may develop data-intensive practices without always possessing adequate awareness of the privacy implications (Krein and Schiefner-Rohs 2021). Teachers and administrators may also assume that privacy and security are technical matters belonging to information-technology departments or external vendors. This institutional fragmentation can create accountability gaps.

The procurement stage is therefore one of the most important points of intervention. Before adopting an educational platform, schools should evaluate what categories of student information the system collects, which functions require each category, where information is stored, how long it is retained, who can access it, whether information is transferred to third parties, whether it is used for profiling, and what happens when the contractual relationship ends. Research concerning

Australian schools demonstrates that evaluating EdTech privacy practices can be difficult because digital products often involve opaque and rapidly changing data practices (Harrison et al. 2024). A school should not purchase a platform merely because it provides pedagogical functionality. Privacy impact and children's rights should be part of the procurement assessment itself.

Contracts with technology providers should translate these principles into enforceable obligations. A school-provider agreement should identify the purposes of processing, categories of data, permitted processing activities, retention periods, security obligations, restrictions on subcontracting, procedures for responding to incidents, deletion requirements, audit rights, and mechanisms for terminating unauthorized processing. The provider should not be permitted to repurpose educational data for advertising or unrelated commercial profiling without an independent legal basis and appropriate safeguards. Recent research on commercial EdTech emphasizes that public education systems can become dependent on private digital infrastructures while retaining insufficient bargaining power over data governance (Rivera-Vargas, Raffaghelli, and Mico-Puigcercys 2024). The legal relationship should therefore be structured around the protection of children's rights rather than merely the delivery of software.

Cybersecurity is equally central. Privacy protection is ineffective if schools collect data responsibly but fail to secure the resulting databases. Student information systems may contain identity information, academic records, family information, health-related information, and behavioral records. A breach can expose children to identity theft, harassment, discrimination, or long-term reputational harm. Indonesian research on technology-based educational management has identified weaknesses such as insufficient security technologies, limited backup practices, and inadequate user awareness as continuing challenges (2025). Similar international research shows that educational platforms can vary significantly in encryption, authentication, and cybersecurity practices. Security must therefore be treated as an institutional governance obligation rather than an optional technical enhancement.

Data retention requires comparable scrutiny. Educational institutions frequently retain records because they may be useful for administrative, legal, historical, or pedagogical purposes. However, indefinite retention creates risks when information originally collected for a limited purpose becomes available for unrelated future uses. The longer information remains in digital systems, the greater the potential exposure to unauthorized access, breaches, profiling, and function creep. Data governance should therefore establish retention schedules linked to legitimate educational purposes. When the purpose expires, information should be securely deleted, anonymized where appropriate, or retained only where another clear legal obligation justifies continued storage. De-identification itself, however, should not automatically be treated as sufficient protection because research has demonstrated that supposedly de-identified educational data can sometimes be re-

identified by linking datasets with other publicly available information (Yacobson et al. 2021).

Teachers also have a significant role in privacy governance. Teachers are often the people who directly enter, interpret, share, and act upon student data. Yet research has shown that educators may not always consider who can access student information or how digital data may be exploited by third parties. This creates a need for institutional privacy literacy. Teachers should understand not only technical security practices but also the principles of necessity, proportionality, purpose limitation, confidentiality, and non-discrimination. A teacher should be able to distinguish between information that is educationally necessary and information that is merely interesting or technically available. Such professional judgment is essential because privacy cannot be protected through software settings alone.

The responsibility of educational technology providers should correspondingly include privacy-by-design and security-by-design. Providers should minimize default collection, provide understandable privacy information, restrict employee access, encrypt sensitive data, maintain strong authentication, monitor unauthorized activity, conduct security testing, and establish clear incident-response procedures. Providers should also design systems to prevent unnecessary profiling of children. Where artificial intelligence or learning analytics are used, providers should document the purposes of algorithms, categories of data used, meaningful limitations, and procedures for challenging erroneous or harmful outcomes. Such obligations are increasingly important as EdTech platforms move from simple content delivery toward predictive and adaptive systems.

Toward a Child-Rights-Based Governance Framework for Indonesian Digital Education

A child-rights-based governance framework should begin by recognizing that children's privacy is not an obstacle to educational innovation. Rather, privacy is a condition under which educational technology can be legitimate and sustainable. The best interests of the child should operate as a substantive principle in technology procurement, data processing, algorithmic design, and institutional decision-making. This requires authorities and schools to ask whether a proposed technological practice improves education without imposing disproportionate risks on children's dignity, autonomy, safety, or future opportunities. UNICEF's guidance on data governance in EdTech similarly emphasizes that educational technology creates opportunities for learning while simultaneously producing risks of privacy violations, profiling, and commercial exploitation (UNICEF 2025).

The first substantive principle should be data minimization. Schools should collect only information reasonably necessary for clearly defined educational purposes. A platform's technical capacity to collect data should never be confused with legal or educational necessity. If attendance can be recorded without

continuous location tracking, location tracking should not become the default. If academic progress can be evaluated without recording unrelated browsing behavior, such monitoring should be avoided. If a digital assignment does not require biometric information, biometric collection should not be introduced merely because the technology is available. This principle is particularly important for children because excessive collection can create permanent digital profiles from educational activities that children have little practical ability to avoid.

Purpose limitation should operate alongside minimization. Every significant category of student data should have an identifiable purpose, and that purpose should be communicated in language appropriate to parents, teachers, and students. Data collected for educational administration should not automatically become available for commercial research, targeted advertising, behavioral experimentation, or unrelated profiling. Where a new purpose emerges, the school should conduct a new legal and rights assessment rather than treating the original collection as unlimited authorization. The distinction between primary and secondary use is particularly important because educational data can acquire commercial value as datasets become larger and more predictive. The recent literature on children's data governance demonstrates that commercial EdTech can generate tensions between educational objectives and corporate interests (Lindh and Nolin 2016; Hillman 2022).

Transparency should also be redesigned for children. Conventional privacy policies are often lengthy, legalistic, and written primarily to protect institutions rather than inform young users. Children's privacy notices should be layered, concise, visual where appropriate, and age-sensitive. They should explain what information is collected, why it is needed, who receives it, how long it is kept, and what happens if a breach occurs. Parents and guardians should receive more detailed information, while students should receive explanations appropriate to their age and developmental capacity. Research on privacy literacy indicates that children can improve their understanding of data practices when privacy education is appropriately designed (Desimpelaere, Hudders, and Van de Sompel 2020). Yet education about privacy should complement—not replace—institutional responsibility.

Meaningful participation should form another pillar of the governance model. Children should not be treated only as recipients of protection; they should be given appropriate opportunities to express views about technologies that significantly affect their educational experiences. This principle is particularly relevant where schools introduce surveillance technologies, automated assessment, learning analytics, or monitoring systems. Children's perspectives can reveal concerns that institutional administrators may overlook, including feelings of constant observation, uncertainty about data use, or fear that digital records will affect future educational opportunities. Research on student attitudes toward learning analytics demonstrates that students value transparency, informed choices, and the ability to understand how their data are used (Ifenthaler and Schumacher 2016; Corrin 2021).

Independent oversight is necessary because schools and technology providers may have incentives to prioritize operational efficiency over privacy protection. Indonesia's data protection framework should therefore be implemented through clear institutional responsibilities, sectoral guidance, auditing mechanisms, and effective enforcement. Schools should maintain records of data-processing activities and conduct privacy and child-rights impact assessments for high-risk technologies. Educational technology providers should be subject to contractual and regulatory scrutiny proportionate to the sensitivity and scale of their processing. Where systems involve biometric identification, continuous monitoring, automated profiling, or large-scale behavioral analysis, enhanced safeguards should apply. The governance model should also provide accessible complaint mechanisms through which parents, guardians, and children can report privacy violations.

Effective remedies are particularly important because children's privacy harms may not be immediately visible. A child whose information has been improperly disclosed may experience consequences months or years later. A predictive educational profile may affect how teachers perceive a student without the student ever knowing that the profile exists. A cybersecurity breach may expose information that remains available on the internet long after the original incident. Remedies should therefore include correction, deletion where legally appropriate, restriction of processing, investigation, notification, and compensation where harm occurs. Students should also be able to challenge inaccurate or unfair algorithmic assessments. A rights-based system cannot be considered complete if children and their families have no practical way to contest institutional or technological decisions.

The final component is institutional accountability. Schools should appoint clearly identified personnel responsible for data protection and should establish internal policies governing collection, access, sharing, retention, and deletion. Teachers and administrative personnel should receive regular training. Technology providers should undergo periodic review rather than being approved once and then left unmonitored. Accessibility, privacy, and security requirements should be integrated into procurement and contract renewal. These measures are consistent with the broader conclusion of research on student privacy: technological solutions alone are insufficient because privacy is simultaneously a legal, organizational, social, and educational problem (Prinsloo, Slade, and Khalil 2022).

Reconciling Educational Innovation with Children's Digital Autonomy

The challenge for Indonesia is not to prevent the use of technology in schools but to prevent technological adoption from becoming an uncontrolled expansion of institutional surveillance. Digital education can improve access, personalize instruction, support students with disabilities, provide rapid feedback, and help educators identify learning difficulties. The legal framework should therefore avoid

a simplistic opposition between privacy and innovation. The more appropriate approach is to require innovation to operate within clearly defined rights-based boundaries. This approach recognizes that the educational value of data is contextual: a particular data point may be useful for one educational purpose while being unnecessary or harmful for another. The legality of processing should consequently depend not only on whether data can produce benefits but also on whether the method of obtaining and using those data is necessary and proportionate.

The proportionality principle is especially important when digital education technologies introduce surveillance capabilities. Continuous monitoring may provide administrators with detailed information about attendance, engagement, or behavior, but increased visibility does not necessarily produce better education. Research on learning analytics demonstrates that technological solutions can generate privacy concerns even when they are designed to improve educational outcomes. Students may perceive extensive monitoring as intrusive and may alter their behavior because they believe that every digital action is being recorded (Jones et al. 2020). For children, this could undermine the educational environment by discouraging experimentation, creativity, and expression. Education requires room for mistakes and development; a permanent digital record of every behavioral deviation may conflict with the developmental nature of childhood.

There is also a risk that data-driven education reinforces inequality. Algorithms trained on historical educational data may reproduce existing disparities if the underlying datasets contain socioeconomic, geographic, linguistic, disability, or gender-related biases. A predictive system that identifies certain children as “high risk” may influence teacher expectations and institutional decisions, potentially creating self-fulfilling outcomes. Research on learning analytics has identified concerns about bias, inequity, and the possibility that automated systems may categorize students in ways that undermine autonomy (Tsai et al. 2021). A child-rights framework should therefore require algorithmic accountability whenever automated systems influence educational decisions. Students should have the right to know when automated analysis is used and should have access to meaningful human review when consequential decisions are based on such systems.

The commercial dimension of EdTech further strengthens the case for stricter governance. Public education systems may enter partnerships with companies whose business models depend upon data collection, analytics, or platform ecosystems. This creates a structural conflict when the educational institution's interest in delivering services overlaps with a company's interest in maximizing data-derived commercial value. Recent research on commercial digital platforms in public education identifies privacy and data-protection challenges arising from the increasing role of private platforms in public schooling (Rivera-Vargas, Raffaghelli, and Mico-Puigcercys 2024). The solution is not necessarily to prohibit private providers but to ensure that contractual and regulatory structures prevent

educational necessity from becoming a mechanism for commercial extraction of children's data.

Indonesia's regulatory development should also be understood as an ongoing process. Law No. 27 of 2022 provides an important foundation, but the rapid development of artificial intelligence, learning analytics, biometric systems, and cloud-based education creates new questions that cannot always be answered through general statutory language. Recent Indonesian legal scholarship has emphasized the need for stronger operational safeguards for children's data and greater harmonization between child protection and personal data regulation (Novanta and Pratami 2022). The enactment of Government Regulation No. 17 of 2025 concerning electronic-system governance for child protection further demonstrates that Indonesian digital governance is moving toward more specific child-oriented regulation. The implementation of this regulatory framework should, however, remain attentive to the particular characteristics of educational environments and should avoid creating unnecessary barriers to legitimate learning activities.

The educational sector therefore requires sector-specific governance that connects personal data protection with pedagogical principles. Data processing should be justified not only by administrative necessity but also by educational value. A system that collects large quantities of behavioral data but provides little demonstrable pedagogical benefit should face heightened scrutiny. Similarly, technologies that create significant privacy risks should be subject to stronger impact assessments before deployment. The educational purpose should be demonstrable rather than rhetorical. This approach would ensure that technology serves learning rather than transforming learning environments into permanent data-generation infrastructures.

The final analytical point concerns the meaning of privacy itself. Privacy should not be conceptualized solely as an individual's ability to conceal information. In educational settings, privacy also concerns the power to determine the appropriate context in which information is seen, interpreted, and acted upon. A student's attendance record may be appropriate for a teacher but not for an advertising company. Academic performance may be relevant to a school administrator but not to a platform provider seeking to develop unrelated commercial profiles. Contextual integrity therefore provides a useful conceptual lens because it emphasizes whether information flows are appropriate to the social context in which they occur (Prinsloo, Slade, and Khalil 2022). This perspective is particularly valuable for schools because educational participation should not automatically authorize every possible use of student information.

Conclusion

The digitalization of education in Indonesia creates substantial opportunities to improve learning, administration, accessibility, and educational decision-making,

but it also transforms children into increasingly visible data subjects. Student information can now be collected continuously through learning platforms, school information systems, online assessments, analytics tools, and digital communication services. The resulting data may reveal not only academic achievement but also behavior, engagement, communication patterns, and inferred characteristics. For children, these practices raise heightened human rights concerns because they involve developing individuals whose capacity to understand and control long-term data consequences is limited. Indonesia's Law No. 27 of 2022 provides an important foundation by giving children's personal data special treatment and requiring parental or guardian consent, but legal recognition alone is insufficient. The protection of children's privacy must extend to the entire data lifecycle, including collection, analysis, sharing, retention, profiling, deletion, and remedy.

A rights-based approach requires schools and educational technology providers to treat children's privacy as a substantive condition of legitimate digital education. Data minimization, purpose limitation, security, age-appropriate transparency, meaningful participation, privacy-by-design, and accountable procurement should become institutional requirements rather than optional ethical practices. Schools should retain responsibility for the processing undertaken by technology providers and should use contracts, audits, impact assessments, and technical safeguards to control third-party processing. Providers should be prevented from treating educational access as an unrestricted source of commercial data. Particular scrutiny is required for biometric systems, continuous monitoring, automated profiling, artificial intelligence, and other technologies capable of producing persistent or sensitive profiles of children.

Ultimately, the objective should not be to choose between children's privacy and educational innovation. The objective is to construct a digital education ecosystem in which innovation operates within the boundaries of children's rights. The best interests of the child should guide decisions about what information is necessary, what purposes are legitimate, how long information should remain available, and what protections must exist when technology fails. Children should be treated not merely as objects of educational data collection but as rights holders whose dignity, developing autonomy, and participation must be respected. If Indonesia can integrate these principles into school governance, technology procurement, platform regulation, and data-protection enforcement, digital education can become a tool for educational inclusion without turning the classroom into an environment of uncontrolled surveillance.

References

- Alier, Marc, Maria Josñ Casac Guerrero, Daniel Amo, Charles Severance, and David Fonseca. 2021. "Privacy and E-Learning: A Pending Task." *Sustainability* 13 (16): 9206. <https://doi.org/10.3390/su13169206>.

- Amin, Rafiullah, Jamil Khan, Shazia Akhtar, and Rustiyana. 2025. "Cybersecurity Challenges in Educational Technology: Protecting Student Data in Digital Learning Platforms." *Journal Emerging Technologies in Education* 3 (4).
- Cahyanto, Iman, Manuel E. Caingcoy, and Andy Sutrisno. 2025. "Protecting Student Privacy in Digital Education: A Systematic Review of Wearable Technology Policies in Southeast Asia." *Tarbawi: Jurnal Keilmuan Manajemen Pendidikan* 11 (3).
- Corrin, Linda. 2021. "Shifting to Digital: A Policy Perspective on 'Student Perceptions of Privacy Principles for Learning Analytics.'" *Educational Technology Research and Development* 69 (1): 353–356. <https://doi.org/10.1007/s11423-020-09922-x>.
- Currier, Chad. 2021. "Unresolved Privacy and Ethics Issues Related to Learning Analytics in Higher Education and Academic Librarianship." *Emerging Library & Information Perspectives* 4 (1). <https://doi.org/10.5206/elip.v4i1.13463>.
- Decuyper, Mathias. 2021. "The Topologies of Data Practices: A Methodological Introduction." *Journal of New Approaches in Educational Research* 10: 1–15. <https://doi.org/10.7821/naer.2021.1.650>.
- Desimpelaere, Laurien, Liselot Hudders, and Dienneke Van de Sompel. 2020. "Knowledge as a Strategy for Privacy Protection: How a Privacy Literacy Training Affects Children's Online Disclosure Behavior." *Computers in Human Behavior* 110: 106382. <https://doi.org/10.1016/j.chb.2020.106382>.
- Francis, Mary, Mejai Bola Mike Avoseh, Karen Card, Lisa Newland, and Kevin Streff. 2023. "Student Privacy and Learning Analytics: Investigating the Application of Privacy within a Student Success Information System in Higher Education." *Journal of Learning Analytics* 10 (3): 102–114. <https://doi.org/10.18608/jla.2023.7975>.
- Handayani, Hilda, Siti Nurkamilah, and Ejen Jenal Mutaqin. 2025. "Peningkatan Peran Teknologi dalam Pengelolaan Data Peserta Didik yang Belum Bisa Diakses oleh Seluruh Pihak Sekolah." *Pendas: Jurnal Ilmiah Pendidikan Dasar* 11 (1).
- Hillman, Velislava. 2022. "Data Privacy Literacy as a Subversive Instrument to Datafication." *International Journal of Communication* 16.
- Hoel, Tore, and Weiqin Chen. 2018. "Privacy and Data Protection in Learning Analytics Should Be Motivated by an Educational Maxim—Towards a Proposal." *Research and Practice in Technology Enhanced Learning* 13: 20. <https://doi.org/10.1186/s41039-018-0086-8>.
- Hwang, Soo-Yeon, and Michael Hanson. 2021. "Learning Analytics and Privacy: A Library Perspective." *Internet Reference Services Quarterly* 25 (3): 69–72. <https://doi.org/10.1080/10875301.2021.1946456>.
- Ifenthaler, Dirk, and Clara Schumacher. 2016. "Student Perceptions of Privacy Principles for Learning Analytics." *Educational Technology Research and Development* 64 (5): 923–938. <https://doi.org/10.1007/s11423-016-9477-y>.

- Ilfenthaler, Dirk, and Megan W. Tracey. 2016. "Exploring the Relationship of Ethics and Privacy in Learning Analytics and Design: Implications for the Field of Educational Technology." *Educational Technology Research and Development* 64 (5): 877–880. <https://doi.org/10.1007/s11423-016-9480-3>.
- Jones, Kyle M. L. 2019. "Learning Analytics and Higher Education: A Proposed Model for Establishing Informed Consent Mechanisms to Promote Student Privacy and Autonomy." *International Journal of Educational Technology in Higher Education* 16: 24. <https://doi.org/10.1186/s41239-019-0155-0>.
- Jones, Kyle M. L. 2020. "A Matter of Trust: Higher Education Institutions as Information Fiduciaries in an Age of Educational Data Mining and Learning Analytics." *Journal of the Association for Information Science and Technology*. <https://doi.org/10.1002/asi.24327>.
- Jones, Kyle M. L., Andrew Asher, Abigail Goben, Michael R. Perry, Dorothea Salo, Kristin A. Briney, and M. Brooke Robertshaw. 2020. "'We're Being Tracked at All Times': Student Perspectives of Their Privacy in Relation to Learning Analytics in Higher Education." *Journal of the Association for Information Science and Technology* 71 (9): 1044–1059. <https://doi.org/10.1002/asi.24358>.
- Kamal, Sep Arinda Risa, Desi Rahmawati, Siti Zulaikha, and Syafaat Ariful Huda. 2025. "Transforming Student Data Governance through a Web-Based Management Information System (MIS): A Systematic Literature Review." *Journal of Educational Sciences* 10 (3): 416–426.
- Korir, Maina, Sharon Slade, Wayne Holmes, Yingfei Hūliot, and Bart Rienties. 2023. "Investigating the Dimensions of Students' Privacy Concern in the Collection, Use and Sharing of Data for Learning Analytics." *Computers in Human Behavior Reports* 9: 100262. <https://doi.org/10.1016/j.chbr.2022.100262>.
- Krein, Uwe, and Mandy Schiefner-Rohs. 2021. "Data in Schools: (Changing) Practices and Blind Spots at a Glance." *Frontiers in Education* 6: 672666. <https://doi.org/10.3389/feduc.2021.672666>.
- Marín, Victoria I., and Gemma Tur. 2023. "La Privacidad de los Datos en Tecnología Educativa: Resultados de una Revisión de Alcance." *Edutec. Revista Electrónica de Tecnología Educativa* 83. <https://doi.org/10.21556/edutec.2023.83.2701>.
- Mutumukwe, Chantal, Olga Viberg, Lena-Maria Oberg, and Teresa Cerratto-Pargman. 2022. "Students' Privacy Concerns in Learning Analytics: Model Development." *British Journal of Educational Technology* 53. <https://doi.org/10.1111/bjet.13234>.
- Novanta, Nabella Maharani, and Bunga Desyana Pratami. 2022. "Legal Formulation Policy on the Privacy Protection of Children and Persons with Disabilities in Indonesia." *Asian Journal of Law and Humanity* 2 (2). <https://doi.org/10.28918/ajlh.v2i2.4>.

- Pangrazio, Luci, Neil Selwyn, and Bronwyn Cumbo. 2023. "Tracking Technology: Exploring Student Experiences of School Datafication." *Learning, Media and Technology* 48.
- Potgieter, Isak. 2020. "Privacy Concerns in Educational Data Mining and Learning Analytics." *The International Review of Information Ethics* 29. <https://doi.org/10.29173/irie384>.
- Prinsloo, Paul, and Sharon Slade. 2013. "Learning Analytics: Ethical Issues and Dilemmas." *American Behavioral Scientist* 57 (10): 1510–1529. <https://doi.org/10.1177/0002764213479366>.
- Prinsloo, Paul, Sharon Slade, and Mohammad Khalil. 2022. "The Answer Is (Not Only) Technological: Considering Student Data Privacy in Learning Analytics." *British Journal of Educational Technology* 53. <https://doi.org/10.1111/bjet.13216>.
- Prinsloo, Paul, Sharon Slade, and Mohammad Khalil. 2023. "Multimodal Learning Analytics—In-Between Student Privacy and Encroachment: A Systematic Review." *British Journal of Educational Technology* 54. <https://doi.org/10.1111/bjet.13373>.
- Rivera-Vargas, Pablo, Juliana Raffaghello, and Raquel Mico-Puigcercys. 2024. "Plataformas Digitales Comerciales en la Educaci3n P3blica. Desaf3os Emergentes sobre Privacidad y Protecci3n de Datos." *EduTec. Revista Electr3nica de Tecnolog3a Educativa* 87. <https://doi.org/10.21556/edutec.2024.87.3063>.
- Walker, Kristen L. 2023. "Compulsory Technology Adoption and Adaptation in Education: A Looming Student Privacy Problem." *Journal of Consumer Affairs*. <https://doi.org/10.1111/joca.12506>.
- Wikutomo, Prakoso, Fauzan Hamsyah Permana, and Muhammad Hari Perdhana. 2025. "Perlindungan Anak terhadap Aksesibilitas Internet Berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi." *Journal Equitable* 10 (2).
- Williamson, Ben, Luci Pangrazio, and Neil Selwyn. 2023. "Who Controls Children's Education Data? A Socio-Legal Analysis of the UK Governance Regimes for Schools and EdTech." *Learning, Media and Technology*. <https://doi.org/10.1080/17439884.2022.2152838>.
- Wollny, Sebastian, et al. 2023. "Students' Expectations of Learning Analytics across Europe." *Journal of Computer Assisted Learning*. <https://doi.org/10.1111/jcal.12802>.
- Yacobson, Elad, Orly Fuhrman, Sara HersHKovitz, and Giora Alexandron. 2021. "De-Identification Is Insufficient to Protect Student Privacy, or—What Can a Field Trip Reveal?" *Journal of Learning Analytics*. <https://doi.org/10.18608/jla.2021.7353>.

Legal and International Sources

- Committee on the Rights of the Child. 2021. *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*. CRC/C/GC/25.
- Indonesia. 1945. *The Constitution of the Republic of Indonesia of 1945*.
- Indonesia. 2002. *Law No. 23 of 2002 concerning Child Protection*, as amended.
- Indonesia. 2019. *Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions*.
- Indonesia. 2022. *Law No. 27 of 2022 concerning Personal Data Protection*.
- Indonesia. 2025. *Government Regulation No. 17 of 2025 concerning Governance of Electronic System Implementation for Child Protection*.
- United Nations. 1989. *Convention on the Rights of the Child*.
- UNICEF. 2019. *Children and Online Privacy*.
- UNICEF. 2024. *Data Protection in Schools: Guidance for Legislators, Policy Makers and Schools*.
- UNICEF. 2025. *Data Governance for EdTech: Landscape Review and Policy Recommendations*.

Acknowledgment

None

Funding Information

None

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement

N/A