

DIGITAL PRIVACY RIGHTS IN EDUCATIONAL TECHNOLOGY PLATFORMS

Dr. Riya Malhotra

Assistant Professor

Department of Educational Technology and Digital Policy

School of Education

University of Digital Studies, Bengaluru, Karnataka, India

Abstract

Educational technology platforms now mediate classroom teaching, assessment, communication, tutoring, attendance, content delivery, and learning analytics. Their usefulness, however, depends on extensive processing of learner information, including identity details, academic records, interaction logs, device data, audio and video streams, behavioural indicators, and, in some cases, biometric or inferred information. This paper presents a comparative, evidence-based analysis of digital privacy rights in educational technology platforms. It examines how privacy risks arise across learning management systems, videoconferencing tools, AI-enabled tutoring systems, online assessment and proctoring services, mobile learning applications, and collaborative classroom platforms. The analysis draws on privacy scholarship, educational technology research, international guidance, and regulatory principles; it does not claim an original survey or experiment. Privacy is assessed through the lenses of data minimisation, purpose limitation, meaningful notice, consent and choice, access and correction, deletion and retention controls, security, non-discrimination, transparency of automated decision-making, and institutional accountability. The study finds that educational settings create a distinctive privacy context because students often cannot freely avoid a platform selected by a school or university, and younger learners may have limited capacity to understand long privacy notices. High-risk functions include continuous behavioural tracking, predictive profiling, AI-generated inferences, remote proctoring, third-party advertising technologies, and indefinite retention of learner data. The paper concludes that digital privacy in education should be treated as a condition of equitable learning rather than as a secondary technical issue. Effective protection requires privacy-by-design, child- and learner-centred safeguards, transparent vendor contracts, independent oversight, educator training, and accessible remedies for students and families.

Keywords: Educational Technology, Digital Privacy, Student Data, Learning Analytics, Artificial Intelligence in Education, Online Proctoring, Data Governance, Child Rights, Platform Accountability, Privacy by Design

1. INTRODUCTION

Educational technology has become part of the ordinary infrastructure of schooling and higher education. Learning management systems distribute readings and assignments; video platforms host live classes; assessment tools capture submissions and grades; adaptive applications recommend content; messaging systems enable teacher-student communication; and AI tools increasingly respond to learner prompts or generate feedback. Each service can support participation, continuity, and personalised learning. At the same time, each service may create a record of how a learner studies, communicates, performs, attends, interacts, and responds to automated systems. These records can reveal more than academic

achievement. They may expose learning difficulties, interests, disabilities, language preferences, family circumstances, patterns of attention, and other sensitive aspects of a student's life.

Digital privacy rights in education therefore concern more than secrecy. They involve the conditions under which learner information is collected, interpreted, shared, stored, secured, corrected, and deleted. A student should not have to surrender unnecessary personal information merely to attend class, submit work, or receive feedback. A teacher should not be required to rely on opaque tools that make significant recommendations without explaining their data practices. Parents and educational institutions also need reliable ways to understand which organisations receive

student data and for what purpose. In this sense, privacy is closely connected to autonomy, dignity, equality, freedom of expression, and trust in the educational relationship.

The structure of the educational technology market can complicate these expectations. Schools and universities may deploy multiple products at the same time, often combining services from platform providers, cloud-hosting companies, analytics vendors, identity-management systems, payment processors, and third-party integrations. A single learning activity can therefore involve an ecosystem rather than one platform. If responsibilities are unclear, students and families may be unable to identify who holds their information, whether it is used to build profiles, how long it is retained, or how they can seek redress after a breach or an unfair automated outcome.

The challenge is especially important for children and other learners with reduced bargaining power. In many situations, participation in an educational platform is not voluntary in a meaningful sense because the platform is required by a course, school, or examination process. Long and technical terms of use cannot by themselves create genuine understanding or protect vulnerable users. Effective governance must account for the dependency created by institutional choice, the educational purpose of the service, the sensitivity of the information involved, and the possible consequences of data-driven decisions.

This study analyses privacy rights across major categories of educational technology platforms. It identifies the main data pathways, compares risk profiles, and outlines responsibilities for vendors, educational institutions, educators, policymakers, and learners. The purpose is to frame privacy as a central element of a safe and inclusive digital learning environment rather than as a matter left only to individual settings and consent screens.

2. LITERATURE REVIEW

Privacy scholarship has long emphasized that privacy is not simply an individual preference

to conceal information. Nissenbaum's contextual integrity approach explains that information practices should remain appropriate to the social context in which data are shared. Education is a context with distinctive expectations: learners disclose information to receive instruction, assessment, feedback, and support, not to become subjects of commercial surveillance or unrestricted behavioural profiling. This perspective is useful because it directs attention to whether data flows remain connected to a legitimate educational purpose.

Research on learning analytics has further demonstrated the need for clear ethical principles. Scholars have highlighted the tension between legitimate efforts to identify students who need support and the risks of monitoring, labelling, prediction, and exclusion. Data that may appear harmless in isolation can become sensitive when combined, especially when a platform derives inferences about engagement, ability, attention, or future performance. The concern is not that analytics should never be used; rather, platforms and institutions must demonstrate that the use is necessary, proportionate, understandable, and subject to human review.

Policy guidance has increasingly addressed the governance of online learning. UNESCO materials on personal data protection in online education stress the importance of lawful and secure processing, while recent child-rights guidance has called for stronger oversight of educational technology used in schools. Regulatory frameworks such as the GDPR, FERPA, and COPPA provide different legal approaches, but they share important themes: protection of personally identifiable information, limits on unnecessary disclosure, accountability for organisations handling data, and special attention to children. The following table summarises selected contributions that inform the present analysis.

LITERATURE REVIEW SUMMARY TABLE

S. No.	Author / Year	Study Focus	Key Contribution	Limitations Identified
1	Nissenbaum	Contextual	Explains privacy as	Does not focus

	(2010)	integrity and privacy norms	appropriate information flow within social contexts	specifically on current EdTech platform ecosystems
2	Slade & Prinsloo (2013)	Ethics of learning analytics	Identifies consent, transparency, and power asymmetry as central concerns	Written before the widespread use of generative AI tools
3	Pardo & Siemens (2014)	Ethical and privacy principles for analytics	Sets out transparency, student control, security, and accountability principles	Focuses primarily on analytics rather than all types of learning platforms
4	Regan & Jesse (2019)	Big data and personalised learning	Shows how sorting and tracking can affect fairness and student agency	Emphasis is largely on the United States policy context
5	UNESCO IITE (2020)	Online-learning data protection	Provides practical guidance on privacy and security for learners, teachers, and parents	Guidance is broad and requires local legal adaptation
6	UNICEF (2024)	Data protection in schools	Links platform governance to children's rights and institutional oversight	Does not replace jurisdiction-specific compliance requirements

3. OBJECT OF STUDY

The primary focus of this research is to examine how digital privacy rights operate within educational technology platforms and how those rights may be weakened or strengthened by platform design, procurement practices, data governance, and institutional oversight. The study addresses student, parent, educator, and institutional interests while recognising that learners are the principal subjects of many education-related data flows. The objects of study are outlined below:

3.1 EDUCATIONAL TECHNOLOGY PLATFORMS UNDER INVESTIGATION

- Learning management systems used for course delivery, assignments, grading, attendance, and student communication
- Video-conferencing and virtual-classroom services that process audio, video, chat, attendance, and participation data
- AI-enabled tutoring, adaptive learning, recommendation, and learning-analytics platforms
- Online assessment, plagiarism-detection, identity-verification, and remote-proctoring services
- Mobile learning applications, digital textbooks, classroom collaboration tools, and student portals

3.2 LEARNER DATA AND PRIVACY CONTEXTS

- Identity, contact, enrolment, attendance, grade, assignment, and course-progression information
- Interaction data such as clicks, time-on-task, reading patterns, discussion posts, prompts, and submitted work
- Technical data including device identifiers, IP addresses, cookies, browser characteristics, and location indicators
- Sensitive or high-impact data such as audio, video, biometric templates, disability-related information, and behavioural inferences
- Data shared through integrations, cloud storage, advertising technologies, payment services, and third-party analytics

3.3 PRIVACY RIGHTS EVALUATION PARAMETERS

- Legitimacy, necessity, and proportionality of data collection for a stated educational purpose
- Clarity and accessibility of notices, including age-appropriate explanations for children and families
- Access, correction, deletion, portability, and retention controls for learners and authorised representatives
- Restrictions on secondary use, targeted advertising, sale, profiling, and sharing outside the educational context

- Security safeguards, breach notification, human oversight, complaint pathways, and effective remedies

3.4 COMPARATIVE ANALYSIS FOCUS

- Differences between routine instructional tools and high-intrusion monitoring or assessment systems
- The relationship between platform functionality, data sensitivity, and the practical ability of students to refuse or opt out
- Institutional responsibilities in vendor selection, contract governance, staff training, and lifecycle management
- The effect of AI-driven inference, automated recommendations, and predictive modelling on student agency and fairness

3.5 RESEARCH OBJECTIVE SCOPE

- To map the principal privacy risks associated with major categories of educational technology platforms
- To explain how platform design and data governance influence learner rights and educational trust
- To identify gaps in consent, transparency, data minimisation, retention, security, and redress mechanisms
- To recommend practical safeguards for privacy-respecting digital learning environments

4. RESEARCH METHODOLOGY

The present study adopts a comparative and evidence-based research methodology. It synthesises academic literature on privacy, learning analytics, and educational technology; international guidance on online learning and child data protection; and widely recognised regulatory principles relevant to student information. The research does not present a new survey, audit, experiment, or statistical dataset. Instead, it evaluates how different educational technology functions create distinct categories of privacy risk and how governance controls can reduce those risks.

The analysis follows the learner-data lifecycle. It considers how information is collected at registration or through routine platform use, how it is linked to course activity and device data, how it is transformed into profiles or recommendations, how it may be shared with service providers, and how it is retained or

deleted after a course ends. Each platform category is assessed under common dimensions: data sensitivity, necessity, user awareness, ability to exercise choice, transparency of automated processing, exposure to third parties, security requirements, and availability of remedies.

The methodology also recognises that privacy effects are not evenly distributed. Children, students with disabilities, learners using shared devices, users with limited digital literacy, and students subject to high-stakes assessment may face additional vulnerability. The study therefore distinguishes between ordinary instructional data and information that can materially affect dignity, access, opportunity, or educational outcomes.

METHODOLOGY FRAMEWORK

1. The study uses a qualitative comparative design covering major educational technology platform categories.
2. Academic scholarship, international guidance, privacy principles, and regulatory materials support the analysis.
3. The assessment considers instructional, technical, behavioural, biometric, and inferred forms of learner data.
4. Platform functions are compared according to data sensitivity, intrusion level, and the possibility of meaningful student choice.
5. Data minimisation, purpose limitation, transparency, security, retention, and redress are treated as core evaluation criteria.
6. Automated recommendations, predictive analytics, and AI-generated inferences are assessed for explainability and human oversight.
7. The analysis distinguishes legal compliance from broader ethical obligations owed to students and families.
8. Institutional procurement, vendor contracts, staff practices, and platform design are considered shared governance responsibilities.
9. No fabricated prevalence figures, breach counts, or survey results are presented.
10. Recommendations emphasise prevention, learner participation, accessible rights, and accountable platform governance.

5. DATA ANALYSIS

The data analysis section presents a comparative evaluation of privacy rights across educational technology platforms. The analysis is based on the typical functions of these platforms, the types of information they may process, the potential consequences of misuse or overcollection, and the practical safeguards available to learners and institutions. It does not assume that all tools create the same level of risk. A platform used to distribute a reading may require a very different privacy assessment from a remote-proctoring service that records a student's room, face, voice, device processes, and examination behaviour.

Six platform settings are considered: learning management systems, video-conferencing tools, AI tutoring and learning-analytics services, online assessment and remote-proctoring systems, mobile and app-based learning services, and classroom collaboration platforms. The comparison is qualitative because risk depends on contractual terms, local law, age of users, platform configuration, data-retention practices, integration choices, security controls, and the educational consequences of refusing a service.

5.1 COMPARATIVE PRIVACY RIGHTS ANALYSIS

S. No.	Platform Category	Primary Data Processed	Main Privacy Concern	Rights and Safeguards Needed	Risk Level	Priority
1	Learning management systems	Identity, enrolment, assignments, grades, attendance, activity logs	Excessive retention, hidden analytics, unclear third-party integrations	Data inventory, role-based access, retention limits, access and correction rights	High	Immediate
2	Video-conferencing and virtual classrooms	Audio, video, chat, attendance, screen shares, recordings	Unnecessary recording, exposure of home environments, sharing of class content	Recording controls, default privacy settings, clear notice, secure storage and deletion	High	High
3	AI tutoring and learning analytics	Responses, prompts, performance patterns, behavioural data, inferred profiles	Opaque profiling, bias, automated labelling, reuse for model training	Purpose limitation, explanation, human review, opt-out alternatives, independent evaluation	Very High	Immediate
4	Online assessment and remote proctoring	Identity documents, webcam feeds, room scans, biometrics, device activity	Intrusive surveillance, false flags, discrimination, high-risk retention	Necessity test, less-intrusive alternatives, strict retention, appeal and human review	Very High	Immediate
5	Mobile learning apps and digital	Device identifiers, cookies,	Tracking beyond educational	Privacy-by-default, no behavioural	High	High

	textbooks	location indicators, usage analytics	need, advertising technologies, weak child protections	advertising, SDK review, child-centred notices		
6	Classroom collaboration and communication platforms	Messages, files, social interaction data, teacher feedback, group work	Overbroad visibility, unauthorised sharing, data export after course completion	Granular permissions, moderation, secure sharing, controlled archival and deletion	Moderate-High	Important

5.2 EXTENDED DIGITAL PRIVACY RIGHTS EVALUATION

- Learning management systems often become the central repository of a student's educational record. Their design should prevent default collection of information that is not required for teaching, assessment, support, or administration. A clear data inventory is essential because educators and students may not know which analytics features are active, whether records are copied to external services, or how long activity histories remain available after a course ends. Access controls should reflect educational roles rather than provide broad visibility to every administrator or integrated application.
- Video-conferencing tools can bring private spaces into the educational environment. Camera feeds may reveal family members, housing conditions, location cues, religious items, or other personal information that is unrelated to learning. Recording should therefore not be treated as a routine default. Schools and universities should define when recording is necessary, who can access it, whether an alternative learning path is available, and how long a recording is retained. Students should not be pressured to disclose more of their private environment than the learning activity requires.
- AI tutoring and learning-analytics tools may generate inferences that have greater impact than the raw data from which they are produced. A prediction that a student is disengaged, at risk of failure, or likely to need intervention can influence teacher attention, support decisions, or

expectations. Such inferences may be incomplete, inaccurate, or shaped by data that reflect unequal access to devices and connectivity. Learners should be informed when significant recommendations are generated, should be able to question or correct relevant information, and should have meaningful access to human review.

- Online assessment and remote-proctoring systems are among the most intrusive categories because they can combine identity verification, video observation, room scans, audio capture, keystroke analysis, browser monitoring, and automated flagging. A higher educational objective, such as examination integrity, does not remove the need for necessity and proportionality. Institutions should compare less-intrusive alternatives, set strict limits on collected data, prohibit secondary use, provide accessible appeal procedures, and ensure that automated flags are never treated as final proof of misconduct without fair human assessment.
- Mobile applications, digital textbooks, and plug-in tools require particular attention to third-party software development kits, cookies, device permissions, and advertising-related data flows. An application may appear to provide a narrow learning service while sending telemetry to multiple external entities. Procurement review should include technical and contractual checks for tracking technologies, not only a reading of the vendor's public privacy policy. Platforms used by children should avoid behavioural advertising, sale of learner data, or designs that pressure users to

disclose more information than is necessary.

- Collaboration platforms create records of student speech, peer interaction, and teacher feedback. These records can support teamwork, but they can also make students feel continuously visible and reduce willingness to participate. Privacy-respecting design should give educators options to control audience scope, manage file-sharing permissions, set reasonable archiving periods, and protect group work from unnecessary redistribution. Students should be taught how to use these controls, and institutions should provide a trusted channel for reporting privacy concerns or harmful sharing.

5.3 OBSERVATIONS FROM DATA ANALYSIS

- Privacy risk is function-specific: ordinary course administration may require limited records, while proctoring, AI profiling, and biometric verification create much higher intrusion.
- Educational dependence weakens the assumption that students can freely consent to every platform practice; rights must therefore be supported by institutional safeguards, not only by user choice.
- The most significant harms may arise from derived information, automated inferences, and cross-platform data linkage rather than from a single data field collected at registration.
- A public privacy policy is not sufficient evidence of protection. Institutions need data maps, vendor due diligence, contract controls, configuration review, and regular monitoring.
- Security is necessary but not sufficient. A platform can be technically secure while still collecting unnecessary data, retaining it indefinitely, or using it for purposes students reasonably did not expect.
- Meaningful privacy rights require accessible notices, practical request processes, timely deletion, and non-retaliatory alternatives when a learner raises a legitimate concern.
- Educators need support to make privacy-aware decisions because classroom

settings, optional features, and integration choices can materially change the information exposed to a platform.

6. DISCUSSION

The comparative analysis demonstrates that privacy in educational technology is shaped by the design of learning systems, not merely by the willingness of users to read terms and conditions. Educational institutions choose platforms, configure features, set participation requirements, and often act as the principal relationship through which students encounter a service. Vendors, in turn, determine default settings, collection practices, data-sharing pathways, retention schedules, and whether sensitive analytics functions are enabled. Privacy governance must therefore recognise a chain of responsibility rather than place the burden on individual students or parents.

A rights-based approach begins with the educational purpose of the platform. Information should be collected only when it is necessary for a clearly stated learning, assessment, support, or administration function. The existence of a technical capability does not automatically justify its use. For example, a platform may be able to record every classroom session, analyse facial behaviour, or track activity across devices, but an institution must still establish whether those functions are appropriate, proportionate, and compatible with learners' expectations. Purpose limitation should continue after initial collection: data obtained for teaching should not be repurposed for advertising, unrelated commercial profiling, or indefinite model training without a valid and transparent basis.

Consent remains important, but it should not be treated as the sole solution. In compulsory or high-stakes educational settings, learners may have little practical ability to refuse a designated platform. A student who declines a privacy-invasive proctoring tool, for example, may risk losing access to an examination unless an equivalent alternative exists. Ethical practice therefore requires institutions to provide meaningful accommodations, accessible support, and a fair process for reviewing concerns. Child-centred design is especially important because children may not fully understand data risks and may be

influenced by interfaces that encourage disclosure or continuous engagement.

AI systems raise additional questions of fairness and explainability. When platforms infer risk, engagement, ability, or behaviour from learner data, the resulting profile can shape educational opportunities even if it is technically described as a recommendation. Inaccurate or biased inferences may disadvantage students who share devices, have intermittent connectivity, use assistive technologies, write in a second language, or engage with learning materials in non-standard ways. Institutions should require evidence that high-impact analytics are valid for the context in which they are used, prohibit solely automated adverse decisions, and ensure that teachers and students can understand and challenge consequential outputs.

Vendor contracts are a crucial but frequently overlooked control. A privacy-respecting contract should define the educational purpose, data categories, security requirements, access restrictions, breach notification duties, subprocessor controls, deletion timelines, audit rights, assistance with learner requests, and limits on secondary use. Public procurement should also consider interoperability and exit planning so that a school is not locked into a vendor that cannot provide data portability or secure deletion. These safeguards transform privacy from a statement of intention into an enforceable operational responsibility.

Finally, privacy protection should support rather than obstruct educational innovation. Students benefit when technology is designed to serve learning without treating them as sources of unrestricted behavioural data. Privacy-by-design can encourage better platform architecture, clearer user interfaces, lower-security risk, and stronger trust between learners, educators, and institutions. The policy goal is not to reject digital tools, but to ensure that their benefits are achieved without normalising surveillance or weakening the rights of those who depend on education.

7. CONCLUSION

This study examined digital privacy rights in educational technology platforms across

learning management systems, virtual classrooms, AI tutoring and learning analytics, online assessment and remote proctoring, mobile learning applications, and classroom collaboration tools. The analysis shows that learner data can include far more than grades and enrolment records. Platforms may collect interaction logs, device information, audio and video, behavioural indicators, biometric signals, and derived profiles that influence educational experience and opportunity. The sensitivity of these data requires safeguards that reflect the distinctive power relationship between institutions, vendors, and learners.

High-risk uses require the strongest controls. Remote proctoring, AI profiling, biometric verification, continuous behavioural tracking, and broad third-party sharing should not be adopted simply because they are technically available. They require necessity assessments, transparent explanation, strict data minimisation, limited retention, independent review, secure alternatives, and fair routes for challenge. Routine platforms also need attention because ordinary classroom tools can become privacy-invasive when data are retained without purpose, combined across services, or shared beyond the educational relationship.

The study concludes that privacy is a shared operational responsibility wherever an institution or vendor collects, processes, interprets, stores, or shares learner information. Effective protection depends on privacy-by-design, age-appropriate notices, no-surveillance default settings, vendor accountability, educator capacity-building, strong security, and accessible student rights. Future research should examine the lived experiences of learners using AI-enabled platforms, the accuracy and equity of educational predictions, the effectiveness of procurement safeguards, and the consequences of data retention after students leave a course or institution. Such work can help ensure that digital learning develops with autonomy, dignity, and trust at its centre.

8. REFERENCES

1. Barocas, S., & Selbst, A. D. (2016). *Big data's disparate impact*. *California Law Review*, 104(3), 671-732.
2. Binns, R. (2018). *Fairness in machine learning: Lessons from political philosophy*. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 149-159.
3. Bulger, M. (2016). *Personalized learning: The conversations we are not having*. Data & Society Research Institute.
4. European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. *Official Journal of the European Union*, L119, 1-88.
5. Federal Trade Commission. (2022). *Policy statement of the Federal Trade Commission on education technology and the Children's Online Privacy Protection Rule*. Washington, DC: FTC.
6. Federal Trade Commission. (n.d.). *Children's Online Privacy Protection Rule (COPPA)*. Washington, DC: FTC.
7. Ifenthaler, D., & Schumacher, C. (2016). *Student perceptions of privacy principles for learning analytics*. *Educational Technology Research and Development*, 64, 923-938.
8. Kwet, M., & Prinsloo, P. (2020). *The "smart" classroom: A new frontier in the securitization of education*. *Learning, Media and Technology*, 45(2), 225-240.
9. Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
10. Pardo, A., & Siemens, G. (2014). *Ethical and privacy principles for learning analytics*. *British Journal of Educational Technology*, 45(3), 438-450.
11. Prinsloo, P., & Slade, S. (2017). *An elephant in the learning analytics room: The obligation to act*. *Proceedings of the Seventh International Learning Analytics and Knowledge Conference*, 46-55.
12. 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, 167-179.
13. Selwyn, N. (2019). *Should robots replace teachers? AI and the future of education*. Polity.
14. Slade, S., & Prinsloo, P. (2013). *Learning analytics: Ethical issues and dilemmas*. *American Behavioral Scientist*, 57(10), 1510-1529.
15. Solove, D. J. (2006). *A taxonomy of privacy*. *University of Pennsylvania Law Review*, 154(3), 477-560.
16. UNESCO. (2023). *Global education monitoring report 2023: Technology in education: A tool on whose terms?* Paris: UNESCO.
17. UNESCO. (2023). *Guidance for generative AI in education and research*. Paris: UNESCO.
18. UNESCO Institute for Information Technologies in Education. (2020). *Personal data and privacy protection in online learning: Guidance for students, teachers and parents*. Moscow: UNESCO IITE.
19. UNESCO Institute for Information Technologies in Education. (2020). *Personal data security technical guide for online education platforms*. Moscow: UNESCO IITE.
20. UNESCO. (2022). *Minding the data: Protecting learners' privacy and security*. Paris: UNESCO.
21. UNICEF. (2024). *Data protection in schools: Guidance for legislators, policy makers and schools*. Geneva: UNICEF.
22. United Nations Committee on the Rights of the Child. (2021). *General comment No. 25 on children's rights in relation to the digital environment*. Geneva: United Nations.
23. U.S. Department of Education. (n.d.). *Family Educational Rights and Privacy Act (FERPA). Protecting Student Privacy*. Washington, DC: U.S. Department of Education.
24. U.S. Department of Education. (n.d.). *Education technology vendors. Protecting Student Privacy*. Washington, DC: U.S. Department of Education.
25. Williamson, B. (2017). *Big data in education: The digital future of learning, policy and practice*. Sage.



26. Williamson, B., Eynon, R., & Potter, J. (2020). *Pandemic politics, pedagogies and practices: Digital technologies and distance education during the coronavirus emergency*. *Learning, Media and Technology*, 45(2), 107-114.