OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

# Protecting the privacy of children and youth through responsible use of educational technologies in the classroom

Federal, Provincial, Territorial (FPT) Privacy Commissioners and Ombuds with responsibility for privacy oversight - November 2025

Resolution

## 1 Context

In Canada, children and youth have the right to both privacy and education. These rights are fundamental and interdependent, as affirmed under international law, including the United Nations Convention on the Rights of the Child (UNCRC) of which Canada is a signatory.

In Canada, education is mandatory from an early age, and today's classrooms increasingly rely on educational technologies and data-driven tools. Educational technologies ("EdTech") are tools specifically developed for teaching and learning environments ranging from major platforms to single-purpose applications. This includes technologies that support curriculum delivery, content engagement, attendance, and testing and assessment of students attending elementary, secondary and post-secondary institutions.

EdTech can enrich learning through interactivity and personalization. It can extend access to education for those living in disadvantaged areas and help support individualized learning needs. It can also enable real time feedback and foster collaboration between students and educators. However, its use in the classroom can also introduce complex privacy risks.

EdTech operates in an environment where public/private partnerships or procurements are the norm, which introduces the risk of data commercialization interests diverting from public education goals. Edtech tools can have weak privacy policies[1] that allow for excessively broad collection of personal information, including information about academic performance, learning abilities, and behaviour during system interactions. The scope of this data collection, often unclear to children, youth, parents and educators, raises concerns about how the personal information of children and youth is being used, stored and potentially shared within and beyond the education context. Typically, children and youth have little to no choice but to engage with the EdTech tools selected and used by their educators, schools, schoolboards and post-secondary institutions. Governments bear responsibility for ensuring that students' best interests, including their privacy, are considered when Edtech tools or systems are assessed and authorized for educational purposes.

Alongside the rapid pace of development and implementation of EdTech tools across the country, we are seeing significant consequences for the privacy of our children and youth when a breach occurs. A powerful demonstration of this was the recent PowerSchool Cyberattack, reported in January 2025, that impacted millions of students across Canada.[2] This incident

1. Veale, M., Schools must resist big EdTech – but it won't be easy, in Livingstone, S., and Pothong, K. (Eds.) (2022) Education Data Futures: Critical, Regulatory and Practical Reflections. Digital Futures Commission, 5Rights Foundation.
2. See Cyberattack affecting school boards across Canada may involve decades of data. What can families do? | Radio-Canada.ca.

is a stark reminder of the critical importance of safeguarding the sensitive personal information of vulnerable children and youth, and not retaining their information any longer than necessary.

As these technologies evolve, additional key risks include:

- **Profiling and inferences:** Artificial intelligence (AI) technologies create new opportunities for personalisation at scale, but also new privacy concerns. For example, based on data such as a child's behaviour, performance, personality, or beliefs, AI can be used to infer sensitive characteristics such as socioeconomic status or mental health, or to make predictions about performance which could impact a child's classroom experience and pre-emptively shape their educational path.
- **Manipulative design:** Deceptive design patterns, such as complex and confusing language, obstruction, and nudging techniques, have been found frequently on websites and apps directed to children and youth in Canada.[3] These can have a negative impact on young people who may not recognize such patterns or grasp the risks and consequences related to their privacy choices online.
- **Biometric surveillance:** Tools that capture biometric data often collect particularly sensitive information without, in many cases, any clear evidence that it is necessary and proportionate for a given educational purpose.[4] For example, this may include test-taking apps that use facial recognition for authentication or AI-enabled proctoring software that monitors eye movement and keystroke patterns to detect certain behaviour.[5]
- **Regulatory gaps:** The extremely rapid pace of developing educational and other related technologies can, and in many instances has, resulted in regulatory gaps due to lagging legislative action and policy responses. Until these regulatory gaps are filled, privacy risks to children and youth in educational settings will only continue to increase.

The EdTech sector spans federal, provincial and territorial (FPT) jurisdictions and involves a diverse range of interested parties across both public and private sectors, including governments, schools and school boards, post-secondary institutions, technology providers, parents or guardians, and children and youth. Canadian privacy regulators are committed to working together to raise awareness of the impacts of EdTech on the privacy rights of children and youth, and to advance consistent privacy-protective approaches for the selection and use of these technologies in classrooms from coast to coast to coast.

**Recalling** the growing national and international recognition of the significant risks to younger generations growing up in a digital environment, and the need to put in place strong and age-appropriate privacy safeguards to protect children and youth in education settings, including:

- The United Nations (UN) General Comment No. 25 on children's rights in the digital environment, which supplements the UNCRC;
- The Organisation for Economic Co-operation and Development (OECD) Council Recommendation on Children in the Digital Environment and Guidelines for Digital Service Providers;
- The G20 Digital Ministers' High Level Principles for Children Protection and Empowerment in the Digital Environment;
- The resolutions of the Global Privacy Assembly on children's rights, including the Resolution on Digital Education for All, the Resolution for the Adoption of an International Competency Framework on Privacy Education, Resolution on e-Learning Platforms and Annex, and the Resolution on Children's Digital Rights;
- UNICEF's Data Governance for EdTech: Policy Recommendations;
- The G7 Data Protection and Privacy Authorities Roundtable Statement;
- The joint Canadian Federal, Provincial and Territorial Privacy Commissioners and Ombuds resolutions, including Putting best interests of young people at the forefront of privacy and access to personal information, Identifying and mitigating harms from privacy-related deceptive design patterns, and Principles for responsible, trustworthy and privacy-protective generative AI technologies.

3. See Resolution on Identifying and mitigating harms from privacy-related deceptive design patterns and 2024 GPEN Sweep on deceptive design patterns.
4. In Québec, express consent is required for biometrics for identification purposes. See Act to establish a legal framework for information technology, sections 44 and 45.
5. See ON IPC, PRIVACY COMPLAINT PI21-00001.

# 2 Therefore

Canada's Federal, Provincial and Territorial Privacy Commissioners and Ombuds with responsibility for privacy oversight (FPT Commissioners) call for the protection and promotion of privacy rights for children and youth as an integral part of their right to education.

FPT Commissioners call on governments, schools, school boards, post-secondary institutions, and EdTech vendors to recognize that the information of children and youth is sensitive, and to ensure that privacy rights and the best interests of the child are paramount in the development, procurement, and deployment of educational technologies.

## We call on federal, provincial, and territorial governments to take the following actions within their respective mandates to:

1. Review, amend or adopt relevant and principles-based privacy legislation to explicitly recognize the sensitivity of children's data and to ensure modern, strong and effective protection of the right to privacy of children and youth in the face of emerging and evolving technologies.
2. In consultation with the privacy regulator in their respective jurisdictions, provide the necessary funding for digital education and privacy training for school boards, administrators, educators, parents and caregivers, and incorporate digital literacy and privacy as part of the standardized school curriculum for children and youth.
3. Establish standard frameworks and assessment criteria for the selection, procurement, and ongoing review of educational technologies. These should include privacy impact assessments and algorithmic impact assessments, where appropriate, for approving and recommending EdTech vendors to schools and school boards.
4. Transparently publish procurement rules for EdTech that demonstrate compliance with privacy laws, including requirements for assessing the tools' validity and reliability, ensuring data integrity and absence of bias, and publicly disclosing how personal information will be collected, used, retained, stored, and deleted.

## We call on school boards, post-secondary institutions, and administrators to:

5. Exercise utmost diligence and engage in responsible privacy protective procurement practices when selecting and contracting with third party EdTech vendors across the full technology lifecycle. This includes first establishing that an EdTech solution is necessary, before proceeding with the various phases of the procurement process, including planning, vendor selection, contracting, agreement management and termination.
6. Deliver and participate in digital education and privacy training for administrators and educators as well as support education among children and youth. This will develop their digital literacy skills, raise awareness about their privacy rights, teach them the basics of AI technologies and how to protect their personal information online in culturally sensitive and age-appropriate ways. Ensure this education is ongoing and supports continual awareness of evolving risks in the digital environment.[6]

6. Practical advice and best practices are provided in Privacy and Access in Public Sector Contracting with Third Party Service Providers | Information and Privacy Commissioner of Ontario. See also the Digital Privacy Charter for Ontario Schools | Information and Privacy Commissioner of Ontario.

7. Consult children, youth and/or their parents or guardians on the selection of EdTech tools to be used in schools and where possible and equitable, consider making available alternatives to EdTech use. Inform them of what personal information is collected, used, retained and disclosed, and notify them of any privacy breaches to help mitigate any negative impacts. Do this in a timely, age-appropriate and understandable manner.
8. Actively listen to students' privacy concerns and consider steps necessary to uphold their rights to participate in decisions that affect them, including their right to access and correct personal information about themselves.
9. When providing Edtech tools to children and youth, ensure that products and services are secure, use privacy protective settings by default, and support the use of pseudonyms and generic logins or anonymous profiles.
10. Establish appropriate retention and deletion policies for personal information collected from students, teachers and parents, retain only necessary information for only as long as required, and monitor compliance.

## We call on EdTech vendors to:

11. Ensure compliance with requirements set out in relevant federal, provincial and territorial privacy legislation. Avoid the collection, use and disclosure of personal information for unfair or harmful purposes.[7]
12. Consider the best interests of the child when designing EdTech, including by:
    - Embedding privacy by design into products and services
    - Following data minimisation principles
    - Ensuring safeguards are proportionate to the sensitivity of collected information
    - Avoiding design practices that would influence, manipulate or coerce users into making decisions that go against their privacy interests
    - Building in appropriate access controls and encryption
    - Establishing privacy settings to their most protective level by default
13. Undertake security testing throughout product lifecycles to confirm the ongoing effectiveness of security measures to protect personal information.
14. Engage children and youth, in meaningful and age-appropriate ways, in the design and evaluation of technologies intended for their use.
15. Use clear and accessible language for all users, especially children and youth, so that they can understand what is being done with their personal information. Vendors should explain:
    - what personal information is being collected and how
    - for what specific purpose(s)
    - what privacy choices are available and how to exercise them without barriers
    - where the data is stored
    - why and with whom it is shared
    - who to contact if they have questions
    - what are the risks and potential harm(s)

7. For examples see OPC Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)

- what will occur in the event of a privacy breach

16. Only collect, use, disclose or retain the personal information of children and youth as is necessary and proportionate for the delivery of educational services. Vendors should not use personal information for secondary purposes such as marketing, product improvement, or AI training without the specific consent of the individual users of their services.
17. Conduct and publish Privacy Impact Assessments (PIAs) that examine the specific risks to children and young people. Where AI systems are used, conduct and publish Algorithmic Impact Assessments prior to deployment or major updates.

## As FPT Commissioners, within the scope of our respective legislative mandates, we commit to:

18. Continue to hold governments, educational institutions and EdTech vendors to account for compliance with relevant privacy laws and regulations in our respective jurisdictions and advocate for adoption of the calls to action in this Resolution.
19. Support governments, educational institutions and EdTech vendors in the responsible design, development, procurement and deployment of privacy-respecting, transparent and accountable EdTech tools and encourage the active involvement of children, youth, and their parents or guardians in the process.
20. Coordinate and collaborate in our collective efforts to educate schools and school boards, post-secondary institutions, administrators, educators, children, youth and their parents or guardians, about the privacy risks of EdTech tools and how to effectively navigate those risks for a safe, secure and responsible digital education experience.

## Special message to children, youth, and their parents or guardians:

Children and youth, you should have agency in the digital world. As you grow and develop, you should be able to express yourselves, explore and navigate the online word, and learn to make your own choices, supported by an informed understanding of how and why your personal information is used. While the primary duty to safeguard your privacy rests with governments, schools, and EdTech vendors, we encourage you and your parents or guardians to advocate for yourselves and your privacy by:

21. Inquiring and engaging in discussions about the educational technologies being used at school, advocating for the use of strong privacy settings, and asking questions about how personal information is being collected, used and disclosed.
22. Through relevant boards, councils and meetings of parents, guardians and students, holding your educational institutions and governments to account for complying with applicable laws and regulations and answering to the calls to action in this Resolution.
23. Making note of who to contact about privacy-related concerns or issues, as they arise, including your school or school board, and the relevant FPT Commissioner in your jurisdiction.