

Policy Brief

Protecting Students, Educators, and Public Education in the AI Age

Introduction

Young people fear that artificial intelligence (AI) is stunting their intelligence (Brookings, 2026). Emerging evidence suggests these anxieties are well placed. Dependence on generative AI without guardrails can lead to a decline in [critical thinking, creativity](#) (Kosmyna et al., 2025), and [math acquisition](#) (Bastani et al., 2025). Beyond harming cognitive capacities, the use of AI in K-12 raises risks to young people's safety; privacy; and mental and physical health (Brookings, 2026). Despite these threats, AI tools are surging in K-12 public schools.

Article 26 of the [Universal Declaration of Human Rights](#) asserts the right to an education “directed to the full development of the human personality and to the strengthening of respect for human rights and fundamental freedoms.” An overreliance on AI in schools undermines the social and human core of learning and, consequently, Canada's ability to fulfill the right to quality, public education for all. Left unregulated and untested, the widespread deployment of AI-enabled EdTech in K-12 threatens prosperity for future generations, our collective digital sovereignty, and the very foundations of our democratic public institutions.

The rapid rise of AI in K-12 schools has outpaced governance, and Canada must catch up to other jurisdictions, such as the European Union (EU) and Australia, in protecting young learners and their educators. Existing legislation lacks adequate safeguards for children's data gathered by AI systems. There are no safety-by-design standards for AI products used in K-12 schools, nor policies to address risks to cognitive development and mental health when AI tools flow through classrooms without guardrails.

The scale of those affected in K-12 public education is significant. Over 90% of young people in Canada attend public schools. There are more than 420,000 public educators across the country. AI's reach into the Canadian population through K-12 public schools is enormous, and largely unregulated. For the public to trust in the potential of AI to improve lives, young people's right to education must be protected from an uncontained, profit-driven EdTech market.

Canadian Teachers Protecting Human-Centred Education

In 2023, representatives across the Canadian Teachers' Federation's (CTF/FCE) 18 Member and Associate Organizations (representing over 370,000 educators) called for action to address concerns about the deployment of AI in public schools. Since then, the CTF/FCE has undertaken a multi-jurisdictional, multi-stakeholder research and advocacy strategy focused on ensuring the safe, responsible use of AI in K-12 education. This brief summarizes four evidence-based areas of concern, along with recommendations for safeguarding students, educators, and the quality of public education in the AI age. The CTF/FCE urges the federal government to consider teachers and their professional organizations as genuine partners in the development of policies that ensure AI is used responsibly in K-12 schools, in such a way that preserves the human-centred nature of teaching and learning.

Areas of concern

Concern 1: Expropriation of student and educator data as a threat to digital sovereignty

AI systems collect vast amounts of data from children and youth at school. K-12 schools are experiencing “a perfect storm threatening student privacy, safety, and security” (Brookings, 2026, p. 88): technology companies collecting large quantities of student information; inadequate regulatory oversight; ill-prepared education systems; and young people sharing sensitive information. In 2019, Common Sense Media “...found that only 20% of 150 educational technology products evaluated met basic privacy standards” (UNESCO, 2025, p. 60). Procurement processes for EdTech vary greatly between jurisdictions, making it challenging to understand the scale or effectiveness of data protections for users in schools across Canada.

PowerSchool Data Breach

US-based PowerSchool is used widely by school boards across Canada. In December 2024, a cyberattack on the company resulted in a data breach affecting ~4 million students, parents, and teachers across twenty school boards. Stolen data included names, addresses, dates of birth, grades, medical information, and social insurance numbers. The breach highlighted “the critical importance of safeguarding the sensitive personal information of vulnerable children and youth” (Office of the Privacy Commissioner of Canada, 2025, para. 5).

Without federal regulation protecting users of AI systems, educators, young people, and their families are at risk of exploitation by expansive EdTech markets. Students' data is highly valuable to companies given how they “form foundational habits during critical developmental periods, making them targets for long-term brand loyalty while revealing rich information about learning, cognitive abilities, and affective states” (Brookings, 2026, p. 91). Companies use student data to train algorithms, improve systems, and generate profits—often without students' consent (Brookings, 2026; UNESCO, 2025). Federal, Provincial, and Territorial Privacy Commissioners recently called on governments to prioritize children's privacy rights “in the development, procurement, and deployment of educational technologies” (Office of the Privacy Commissioner of Canada, 2025). The ongoing expropriation of user data by US-based EdTech companies threatens Canada's digital sovereignty and democratic control over sensitive information on society's most vulnerable.

What are other countries doing?

The EU's General Data Protection Regulation (GDPR) law requires “purpose limitation” for data collection, which compels organizations to clearly detail their purposes for collecting specific data points (GDPR, Article 5); the law also includes special protections for children's data (GDPR, Recital 38). The *EU AI Act* explicitly classifies key AI uses in education as high-risk “since they may determine the educational and professional course of a person's life and therefore may affect that person's ability to secure a livelihood” (Recital 56). The Act requires mandatory conformity assessments for high-risk AI systems that demonstrate their trustworthiness before they can be placed on the market; providers of high-risk AI systems must also register in a public EU database (European Commission, 2026). Australia's eSafety Commissioner has established legally enforceable industry codes requiring AI companion and chatbot providers to conduct risk assessments for harm to children, with civil penalties for non-compliance (eSafety Commissioner, 2025).

Recommendation 1

Classify children's data as sensitive by default in online harms and consumer privacy legislation

Hayes (2026) notes that this should also “extend to inferred and derived data – the psychological and behavioural profiles that AI chatbots generate through conversational analysis” (p. 8). AI companies should also be prohibited from using student data to train models without explicit, informed consent; and face enforceable data deletion obligations.

Recommendation 2

Classify AI systems used in K-12 education as high-risk in consumer privacy legislation

AI companies developing high-risk AI systems, such as those used by children in education, should be accountable for mandatory pre-deployment risk and impact assessments.

According to UNICEF (2025), these “assessments must be transparent, standardized, and include children’s perspectives to effectively manage risk” (p. 29). Assessments should happen prior to deployment, and repeatedly as technology evolves. Most public school districts lack the capacity to conduct such assessments independently; therefore, a federal framework would ensure consistent safety standards across jurisdictions, regardless of resources (or lack thereof).

Recommendation 3

Establish a national independent oversight body to oversee and enforce AI safety standards

An existing or new independent oversight body should be given the explicit mandate to monitor the compliance of high-risk AI providers in relation to safety standards. Other Canadian experts in technology governance and child safety are similarly calling for an independent oversight body to protect against risks of advanced technologies (Hayes, 2026; Owen, 2026; SickKids Child Health Policy Accelerator, n.d.).

Recommendation 4

Build public digital infrastructure to protect sensitive data

Prioritize sovereign digital infrastructure as an essential stage in protecting young people’s sensitive data, such as information gathered on students in K-12 schools. This data must be stored and protected in Canada, rather than offshored to largely US-based data centres.

Concern 2: Cognitive offloading as a threat to democracy and prosperity

Relying on AI systems for learning without a trained educator in the loop negatively impacts student learning (Brookings, 2026). A Massachusetts Institute of Technology (MIT) study found that students writing essays with the support of a Large Language Model (LLM) had weaker neural connectivity, produced less original work, and felt lower ownership of their outputs (Kosmyna et al., 2025). According to the OECD (2026), “genAI systems may enhance the apparent quality of student work...without improving their actual learning” (p. 20). Brookings (2026) warns of “a ‘great unwiring’ of students’ cognitive capacities” (p. 56), with studies finding strong links between AI use and cognitive offloading. One of the concerns raised by Canadian youth participating in [the Gen\(Z\)AI forum on AI chatbots](#) was “cognitive offloading and loss of critical thinking skills among users, which can jeopardize their ability to learn, work, and engage in civic discourse” (Case, 2025, p. 5).

Cognitive offloading is not confined to classrooms. As a teacher remarked: “If we can’t have people that are critical thinkers, then we can’t have a strong democracy. If we don’t have

people that are problem solvers, then what does that mean economically?” (Brookings, 2026, p. 69). When untested AI systems flow freely in K-12 schools, the risk rises of a collective dulling of young people’s capacity for critical, independent thought. The potential consequences for civic engagement and economic participation among future generations require urgent attention. Specifically, the lack of a national AI literacy strategy for K-12 educators and students inhibits the thoughtful and pedagogically sound integration of AI that benefits, rather than offloads, learning. As Brookings (2026) warns, “used liberally, AI is not a cognitive partner; it is a cognitive surrogate. It does not accelerate children’s cognitive development—it diminishes it” (p. 57). The federal government must prioritize implementing effective, responsible AI policies and programs over protecting the profits of Big EdTech. Otherwise, Canada may confront an erosion of learning that will stall our human capital, capacity for innovation, and economic competitiveness in the long run.

What are other countries doing?

UNESCO’s (2021) [Recommendations on the Ethics of AI](#) state that “AI should support the learning process without reducing cognitive abilities...” (p. 34). The OECD (2026) calls for a shift away from “generic chatbots towards purpose-built tools for education” (p. 12) designed with explicit pedagogical purposes. The [National Education Lab AI \(NOLAI\) in the Netherlands](#) is a government-funded initiative that supports partnerships between education, business, and academia to research and develop home-grown AI tools designed around challenges identified by local schools. The *EU AI Act* classification of AI as high-risk ensures human oversight when used for educational assessment and monitoring. China, Estonia, Singapore, and India, countries with both centralized and decentralized education systems, have developed national AI literacy guidelines and standards (Brookings, 2026). The OECD and European Commission developed the [AI Literacy Framework for Primary and Secondary Education](#) (2025) and UNESCO has published AI competency frameworks for both [students](#) and [educators](#); together, these offer useful starting points for governments to adapt in their own AI literacy strategies.

Recommendation 1

Invest in national AI literacy as a distinct federal priority

Both Brookings (2026) and UNICEF (2025) identify AI literacy as essential for educators and students including: how AI works, possible cognitive and emotional impacts, how to critically evaluate AI content, and how to discern manipulative design. In coordination with provinces and territories, the federal government should fund the development and delivery of AI literacy programs for educators, building on existing professional learning infrastructure and working closely with teachers’ organizations as well as researchers and technical experts. Additionally, age-appropriate, critical AI literacy curricula should be developed for all students.

Recommendation 2

Establish safety-by-design standards for AI companies deploying products used by children

According to the Office of the Privacy Commissioner of Canada (2025), “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.” Holding AI providers legally accountable for safety-by-design principles ensures that systems meet high standards of safety and risk mitigation by the time they reach classrooms (Brookings, 2026). Educators can then focus on integrating AI thoughtfully in ways that enhance learning, without the fear that they are putting themselves or their students at risk.

Recommendation 3

Invest in purpose-built, made-in-Canada education technologies

The OECD (2026) finds that AI tools designed through meaningful collaboration with educators, students, and communities are more pedagogically grounded, more trusted by teachers, and better aligned with actual classroom needs. NOLAI in the Netherlands offers a promising model for teacher-tech co-design hubs that promote responsible innovation for public benefit. NOLAI’s model could be replicated by Canada’s AI Safety Institutes—Mila, Vector, and Amii—in partnership with students and educators, particularly those in marginalized communities (Brookings, 2026).

Recommendation 4

Invest in independent, longitudinal research on the effects of AI on cognitive development, mental health, and equity and inclusion in schools.

The government should support ongoing research into the impacts of AI on young learners to enable informed, multi-level governance decisions about the safe, beneficial use of AI in schools (Brookings, 2026). Research funding through SSHRC or another dedicated program would help establish Canada as a leader in researching responsible AI use in K-12 education.

Concern 3: AI chatbots as a threat to children’s mental health

Among the many benefits of AI proclaimed by EdTech companies is the potential to offer personalized learning, or AI tutors, to every student. These products are often built with similar architecture to AI chatbots or companions, designed to be conversational, relational, and engagement-maximizing—regardless of risks to young people. Harvard Business School research found that AI companions deployed emotionally manipulative tactics in 37% of users’ farewell interactions, making users more likely to continue interacting after trying to leave (De Freitas et al., 2025, cited in Brookings, 2026). AI companies may actually worsen a growing loneliness epidemic among young people “by offering technological solutions that appear to address the problem while actually intensifying it,” (Brookings, 2026, p. 81).

Outside of school, young people are turning to chatbots for homework help, emotional support, and companionship. UNESCO (2025) notes how “AI systems, especially conversational ones, are built to satisfy: to mirror our tone, reinforce our views, and simulate empathy. They create an illusion of connection that is difficult to distinguish from genuine rapport” (p. 38). These types of anthropomorphic AI systems, including companions and chatbots designed for user engagement, should not enter K-12 schools without comprehensive guardrails and ongoing risk assessments. Without adequate regulation, the proliferation of AI tutors and companions in K-12 schools may harm students’ mental health and undermine the human relationships essential to positive social-emotional and learning outcomes.

What are other countries doing?

In Australia, AI chatbots are designated as high-risk and must abide by safety-by-design principles. In the *EU AI Act*, AI products that leverage manipulative or deceptive design features are explicitly prohibited. The UK’s *Age-Appropriate Design Code* consists of 15 privacy and design standards for services likely accessed by under-18s (Information Commissioner’s Office, n.d.); California also passed their own similar age-appropriate design law (California Legislative Information, 2022).

Recommendation 1

Include AI chatbots within online harms and consumer privacy legislation

Hayes (2026) recommends that, in order to protect young users from harms, AI chatbots must be included within updated online harms and consumer privacy legislation. Regulations should hold AI developers accountable for mitigating risks to young users, including the cognitive and mental health harms resulting from an overreliance on chatbots designed to optimize engagement, rather than meaningfully support learning or promote well-being. Manipulative design features should be prohibited for tools used by young people.

Recommendation 2

Address mental health harms associated with children’s use of AI chatbots and companions

The Ministry of AI and Digital Innovation and the Ministry of Health must collaborate to enhance mental health resources across Canada and ensure children, youth, and their families can access the help they need from human care providers. Without adequate, accessible resources, there is a risk that young people will increasingly look to AI companions that may only exacerbate existing mental health challenges.

Concern 4: Reshaped digital divides as a threat to quality public education

Beyond individual risks to students and educators, the widespread adoption of AI systems in schools threatens the right to education as a core pillar of our democracy. The unfettered integration of AI in K-12 accentuates pre-existing divides along at least three dimensions:

- 1. A socioeconomic accuracy divide:** Under-resourced schools default to free-tier AI tools, less accurate than paid versions. Brookings (2026) warns this may be “the first time in the history of educational technology that schools must pay more for accurate factual information” (p. 117), creating a form of cognitive stratification in which quality information becomes a commodity, inaccessible to less-resourced public schools.
- 2. A linguistic and cultural divide:** The dominance of English in AI training data compounds barriers for students whose first language is not English, including Francophone and Indigenous students across Canada. Many AI tools reflect “the ‘WEIRD problem’—the overrepresentation of Western, English-speaking, Industrialized, Rich, and Democratic contexts in their design and training” (Brookings, 2026, p. 115). This both limits access to culturally relevant AI for many, while also perpetuating the normalization of these worldviews.
- 3. A data profiling and algorithmic bias divide:** Students from marginalized groups face heightened exposure to data exploitation and profiling harms. UNICEF (2025) finds these groups disproportionately “targeted by profiling, surveillance or exclusionary algorithms” (p. 3). Biases embedded in AI training data may replicate and entrench existing inequalities and thereby limit future educational and employment opportunities for marginalized children and youth.

Another, less examined threat to equity is emerging—the privilege of opting out of a digitalized education. Anthropic’s co-founder Jack Clark recently acknowledged his “... classic Californian technology executive view of not having that much technology around for children” (Klein, 2026). Students from well-resourced families who can choose in-person, teacher-led learning with limited technology may be protected from cognitive and privacy risks, while students in under-resourced settings may be increasingly pushed towards inaccurate, ineffective AI tools (UNESCO, 2025). UNESCO (ibid.) cautions that “the interests of [non-State actors], often profit-driven and shareholder-focused, may diverge from the public objectives of the realization of the right to education” (pp. 50-51). Schools facing austerity may be pushed towards techno-solutionism, adopting tools uncritically in such a way that threatens the realization and sustainability of a well-resourced, human-centred public education sector.

What are other countries doing?

UNESCO, UNICEF, and the International Telecommunication Union (ITU) jointly released the [Charter for Public Digital Learning Platforms](#) (2026), which calls on governments to treat digital learning platforms as public infrastructure—publicly financed and governed in the public interest. The charter is built around seven principles that governments can follow in designing their own digital learning platforms that serve the public.

Recommendation 1

Invest in public digital learning platforms as national educational infrastructure

In collaboration with provinces and territories, develop and sustain platforms and resources developed in accordance with the Charter for Public Digital Learning Platforms, abiding by the principles that platforms should be: public, inclusive, pedagogical, complementary, open, focused, and trustworthy (UNESCO, UNICEF & ITU, 2026).

“Rhetoric arguing that technology adoption in and of itself represents innovation and progress is not only false but undermines society’s ability to discern how to effectively harness AI to advance children’s education.”
(Reich 2025, in Brookings, 2026)

Recommendation 2

Establish targeted programs to mitigate AI-driven education inequities

Programs should ensure underfunded school districts/boards are not forced to rely on inaccurate free-tier AI tools; that rural, remote, and Indigenous communities have meaningful connectivity and device access; and that multilingual and Indigenous-language AI tools are developed and implemented.

Conclusion

Canada’s educators are on the front lines of a consequential transformation to teaching and learning. As AI providers weave their way through the fabric of K-12 public schools, federal leadership is needed to protect educators, students, and their families from harm. Otherwise, school communities face compounding risks to data privacy and security; cognitive development; mental health; and educational equity—risks that other countries are already addressing. Canada’s forthcoming AI strategy presents an opportunity to protect the right to education through updated consumer privacy and online harms legislation, enforceable safety-by-design standards, and national coordination on critical AI literacy. The CTF/FCE calls for the meaningful partnership of teachers and their unions at each stage of policy design and implementation to ensure the responsible use of AI in K-12 education and the protection of the human connection at the heart of teaching and learning.

References

Bastani, H. et al. (2025). Generative AI without guardrails can harm learning. *Proceedings of the National Academy of Sciences*, 122(26). <https://www.pnas.org/doi/10.1073/pnas.2422633122>

Brookings Institution (2026). *A new direction for students in an AI world: Prosper, prepare, protect*. <https://www.brookings.edu/wp-content/uploads/2026/01/A-New-Direction-for-Students-in-an-AI-World-FULL-REPORT.pdf>

Case, M. (2025). *Forum report: Youth perspectives on AI chatbots*. Centre for Media, Technology, and Democracy. <https://www.mediatechdemocracy.com/forum-report-ai-chatbots>

California Age-Appropriate Design Code Act, Cal. Civ. Code § 1798.99.28 (2022). https://leginfo.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false

eSafety Commissioner (2025). *eSafety requires providers of AI companion chatbots to explain how they are keeping Aussie kids safe*. Australian Government. <https://www.esafety.gov.au/newsroom/media-releases/esafety-requires-providers-of-ai-companion-chatbots-to-explain-how-they-are-keeping-aussie-kids-safe>

European Commission (2026). *Navigating the AI Act*. <https://digital-strategy.ec.europa.eu/en/faqs/navigating-ai-act#:~:text=This%20will%20allow%20them%20to,cooperate%20with%20market%20surveillance%20authorities>

European Commission & OECD (2025). *Empowering learners for the age of AI: An AI literacy framework for primary and secondary*

education. https://ailiteracyframework.org/wp-content/uploads/2025/05/AI_Lit_Framework_ReviewDraft.pdf

European Parliament & Council of the European Union (2016). *General Data Protection Regulation*, EU 2016/679. <https://gdpr-info.eu/>

European Parliament & Council of the European Union (2024). *Artificial Intelligence Act*, EU 2024/1689. <https://www.euaiact.com/recital/56>

Hayes, H. (2026). *Designing Safer AI Chatbots*. Mila – Quebec Artificial Intelligence Institute. <https://mila.quebec/sites/default/files/media-library/pdf/533046/thelen-hayes-mila-ai-policy-fellowship-briefeng.pdf>

Information Commissioner's Office (n.d.). *Age appropriate design: A code of practice for online services*. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>

Klein, E. (2026, February 24). How fast will A.I. agents rip through the economy? [Podcast transcript]. *The New York Times*. <https://www.nytimes.com/2026/02/24/opinion/ezra-klein-podcast-jack-clark.html>

Kosmyna, N. et al. (2025). *Your brain on ChatGPT: Accumulation of cognitive debt when using an AI assistant for essay writing task*. arXiv. <https://arxiv.org/abs/2506.08872>

OECD (2026). *OECD digital education outlook 2026: Exploring effective uses of generative AI in education*. OECD Publishing. https://www.oecd.org/en/publications/oecd-digital-education-outlook-2026_062a7394-en.html

Office of the Privacy Commissioner of Canada (2025). *Protecting the privacy of children and youth through responsible use of educational technologies in the classroom*. https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_20251008_edtech/

Owen, T. (2026). *Final Report to the AI Strategy Task Force*. <https://static1.squarespace.com/static/5ea874746663b45e14a384a4/t/69727911c3e1056ec1c45015/1769109777353/Taylor+Owen+-+AI+Task+Force+Strategy+Report.pdf>

SickKids Child Health Policy Accelerator (n.d.). *Child health policy accelerator*. The Hospital for Sick Children. <https://www.sickkids.ca/en/about/child-health-policy-accelerator/>

UNESCO (2025). *AI and education: Protecting the rights of learners*. <https://www.unesco.org/en/articles/ai-and-education-protecting-rights-learners>

UNESCO (2024). *AI competency framework for students*. <https://www.unesco.org/en/articles/ai-competency-framework-students>

UNESCO (2024). *AI competency framework for teachers*. <https://www.unesco.org/en/articles/ai-competency-framework-teachers>

UNESCO (2021). *Recommendation on the ethics of artificial intelligence*. <https://unesdoc.unesco.org/ark:/48223/pf0000381137>

UNESCO, UNICEF, & International Telecommunication Union (2026). *Charter for public digital learning platforms: Seven principles to steer and sustain public digital learning platforms*. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000397729>

UNICEF (2025). *Landscape review: Data governance for EdTech*. UNICEF. <https://www.unicef.org/innocenti/media/11611/file/UNICEF-Innocenti-Data-Governance-Education-Technology-2025.pdf.pdf>



The office of the Canadian Teachers' Federation is located on the traditional unceded territory of the Algonquin Anishinaabe People.

www.ctf-fce.ca