MANITOBA School Boards ASSOCIATION

LEADERSHIP, ADVOCACY AND SERVICE FOR MANITOBA'S PUBLIC SCHOOL BOARDS

28 April 2026

Honourable Mike Moroz
Minister, Innovation and New Technology
Room 314, Legislative Building
450 Broadway
Winnipeg, MB R3C 0V8

[via email only: minint@manitoba.ca]

Re: Bill 51 — *The Public Sector Artificial Intelligence and Cybersecurity Governance Act*

Dear Minister Moroz,

MSBA has been advised by the Clerk to the Standing Committee on Social and Economic Development that our brief regarding Bill 51, *The Public Sector Artificial Intelligence and Cybersecurity Governance Act* was not distributed to the Committee when it met to consider the Bill on 22 April, 2026, due to a technicality.

We therefore convey our insights and observations regarding the Bill to you, under this present correspondence. As no amendments were proposed by us to Bill 51, there is no harm done as a result of the Committee not having received the brief but we did wish to provide some important considerations once the Bill is passed, on behalf of our members.

As you know, MSBA represents the collective voice and interest of Manitoba's 37 publicly elected school boards, as well as the board of the Manitoba Institute of Trades and Technology (MITT), which are entrusted with the governance of public Kindergarten to Grade 12 education for Manitoba children and youth.

MSBA recognizes and acknowledges the Government of Manitoba's underlying and principal objectives of Bill 51:

- to promote responsible, transparent, and accountable use of artificial intelligence (AI) within the public sector, and
- to enhance the cybersecurity posture of public institutions in response to escalating threats.

School divisions share these objectives and are already actively engaged in addressing them through existing statutory obligations, professional regulation, insurance requirements, and sector-specific

governance frameworks. MSBA therefore approaches Bill 51 as an additional safeguard whose ultimate impact will be shaped by the future regulation, standards, and ministerial directives that are presently contemplated, but even more so, could be issued and established under the Bill, once passed.

Our intention will remain that any future regulation, standards and ministerial directives under Bill 51 appropriately reflects the unique context of public education, respects the statutory autonomy of locally elected boards, and includes adequate consultation, funding, and implementation timelines.

Artificial Intelligence holds the transformative potential of enhancing education in the future to a degree previously unforeseen. Our students, staff and schools will inherit learning opportunities not anticipated a generation ago. By the same measure, the public good of AI can only remain good provided adequate safeguards and limitations are placed on the use and development of what is essentially a novel innovation in the consumer market– the impacts, cautions and consequences of which are already being understood based on the generative and agentic tools that are currently available, but with unprecedented opportunity and benefit the more these tools are developed and perfected.

Scope of Bill 51 and Relevance to Public Education

Bill 51 establishes a legislative framework governing the use of Artificial Intelligence systems by prescribed public sector entities, and cybersecurity standards, programs, and incident reporting across the public sector. School divisions are explicitly contemplated as entities that may be prescribed under regulation.

Importantly, the Bill does not itself impose immediate operational requirements on school divisions. Instead, it enables the Government of Manitoba, through regulation, to:

- mandate AI accountability frameworks, transparency measures, and risk assessments;
- set technical standards for AI and cybersecurity;
- require cybersecurity programs, training, and incident reporting; and
- issue entity-specific ministerial directives related to cybersecurity.

It is therefore the future regulatory phase, rather than the enabling statute alone, that raises the most significant implications for public education governance.

Artificial Intelligence in Schools: Balancing Opportunity and Protection

1. **Educational Opportunity and Digital Literacy**

MSBA wishes to emphasize that AI is and shall remain an integral and growing component both of modern public education and of our global economy. At current time, use of AI in Manitoba's classrooms has been very limited. As of the AI Summit convened by the Government of Manitoba in January, 2026, formal use by School Divisions of AI-enabled tools has been confined mainly to

preparation of correspondence alone. In both Canada and the United States, in context of public education and post-secondary education, AI has already been deployed (to name a few critical focus areas) for:

- supporting differentiated learning;
- assisting students with disabilities;
- enhancing language translation and literacy supports;
- streamlining administrative functions;
- conducting teacher and staff evaluations;
- providing classroom and virtual instruction;
- grading and marking academic assignments and examinations;
- providing tutorial and remedial support;
- supporting general research and learning opportunities;
- reviewing admissions documentation and eligibility criteria; and
- preparing students for increasing levels of education and for workforce participation in an AI-enabled economy.

This summarized overview of how AI has been applied is important. The above examples come with significant legal, ethical and moral considerations. The guidance necessary to promote appropriate use of AI is plainly evident from these examples. By the same token, restrictive or overly prescriptive regulation risks undermining equitable access to digital tools, skills and competencies for our staff and students, which are increasingly foundational to professional success, lifelong learning and employability.

2. **Student, Staff, and System Protection**

MSBA has invested considerable effort in understanding the promise and pitfalls of AI for public education. On behalf of our members, we fully acknowledge the need for:

- age-appropriate safeguards and protections;
- human oversight of AI-influenced analysis and decisions;
- protection of student and staff privacy and personal information; and
- mitigation of bias, misuse, misinformation, or unintended educational impacts.

Bill 51's emphasis on transparency, accountability, and risk management aligns in principle with existing educational values and school boards' statutory obligations under FIPPA and PHIA.

3. **Protection of local democracy and institutions**

Public education in Manitoba involves both classroom but also boardroom dimensions. As elected public officials, school boards promote democratic structures, principles and ideals to inform the policy and practices that govern public education. In context of elections in particular, use of AI and/or

destabilization of democracy due to intentional usage of AI, has been amply demonstrated during recent elections held worldwide.

4. **Democracy as a Critical Public Infrastructure**

Elections and democratic institutions constitute critical civic infrastructure, comparable in importance to physical infrastructure, health systems, and financial markets. Their legitimacy depends on:

- public trust in the integrity of electoral processes,
- informed and voluntary participation by voters,
- fairness in political competition, and
- transparency and accountability in decision-making.

Artificial intelligence—particularly generative AI—introduces new capabilities that can amplify, accelerate, and scale threats to each of these democratic foundations, if left ungoverned or misused.

Misinformation, Disinformation, and Deepfakes

Generative AI enables the rapid creation of convincing but false text, audio, images, and video (deepfakes) that can impersonate political candidates, election officials, journalists, or trusted community figures. These tools:

- reduce the cost and skill required to produce misinformation,
- allow malicious actors to tailor messages to specific demographics,
- spread false narratives at scale and speed, and
- undermine voters' ability to distinguish authentic information from fabricated content.

Research confirms that even when deepfake content does not measurably change election outcomes, it erodes public trust, increases polarization, and fuels cynicism about democratic institutions over time.

Foreign and Domestic Interference Amplification

AI can also act as a force multiplier for existing interference strategies used by foreign states, extremist groups, and organized disinformation networks. While such actors have targeted elections for years, AI:

- automates influence operations at unprecedented scale,
- enhances the realism of fake personas and narratives,
- enables rapid adaptation of messaging during critical election periods, and
- facilitates coordinated campaigns across platforms and borders.

National security and election-integrity analyses consistently conclude that AI does not invent entirely new threats but intensifies existing ones, making them harder to detect and counter within limited response windows.

Undermining Trust in Democratic Outcomes

A particularly dangerous feature of AI-enabled misinformation is the creation of a public perception that "nothing can be trusted." When voters are repeatedly exposed to synthetic or manipulated content, they may:

- disengage from civic participation,
- doubt legitimate election results,
- lose confidence in institutions tasked with oversight, and
- become more susceptible to claims of fraud or manipulation, regardless of evidence.

Democratic systems depend not only on accurate outcomes but on collective belief in their legitimacy. AI-driven doubt therefore poses a structural threat even without direct vote tampering.

Election Infrastructure as a Target

Elections, including at the school board level of democracy, rely on complex digital ecosystems, including:

- voter registration databases,
- election-management systems,
- result-reporting platforms,
- communications systems for election officials, and
- public information channels.

AI-enabled cyber tools can increase the sophistication of phishing, social engineering, and automated vulnerability scanning, raising the risk of:

- data breaches,
- service disruption,
- false reporting of results, and
- intimidation or harassment of election workers.

Several public cybersecurity agencies worldwide have emphasized that AI magnifies both the speed and scale of cyber threats, intensifying the need for preparedness, training, and coordinated response protocols.

The Need for Proportionate, Democratic Guardrails

Protecting democracy from AI-related harm again requires careful balance:

- Regulation must be strong enough to prevent abuse,
- Yet restrained enough to protect freedom of expression, freedom of conscience, political debate, satire, and innovation.

Jurisdictions worldwide have learned that overly broad bans or vague standards risk constitutional challenges and public backlash, highlighting the importance of:

- clear definitions,
- risk-based approaches,
- transparency and disclosure requirements, and
- human oversight of high-impact AI uses.

Transparency and Accountability in AI Use

Safeguarding elections equally requires that AI systems used by public institutions, political actors, or platforms be:

- transparent in purpose and function,
- auditable and explainable where they influence democratic processes,
- subject to accountability frameworks, and
- clearly distinguishable from human-created political speech.

Disclosure and watermarking requirements, while imperfect, are increasingly recognized as essential components of democratic resilience.

Education, Digital Literacy, and Democratic Resilience

No regulatory framework alone can fully protect democracy from AI-enabled manipulation. Long-term resilience depends on:

- strong civic education,
- digital and media literacy,
- public awareness of synthetic media risks, and
- trusted, well-resourced public institutions.

Research emphasizes that informed citizens and credible institutions are the most durable safeguard against AI-driven democratic erosion.

MSBA Position on AI Regulation

In context of both the academic and democratic dimensions of public education in Manitoba, MSBA therefore strongly recommends that future regulation under Bill 51:

- Promote clear, sector-specific standards, recognizing that AI in classrooms differs fundamentally from AI in law enforcement, justice, health care, or social services;
- Defer to board autonomy and professional discretion regarding localized approaches to AI implementation;

- Consider the importance of protecting the electoral and structural/institutional processes so necessary and vital for Manitoba's local democracy to flourish.
- Avoid blanket prohibitions or rigid technical prescriptions that may quickly become obsolete in the face of rapidly developing generative and agentic tools and applications; and
- Prioritize educational guidance and capacity-building over compliance-only models.

Cybersecurity Regulation

Current Cybersecurity Expectations in Manitoba Schools

All Manitoba school divisions are already subject to industry-leading and highly rigorous cybersecurity expectations through participation in the Manitoba School Insurance Program (MSI).

As part of this program:

- all school divisions must review and complete comprehensive cybersecurity implementation requirements according to leading industry standards and practices on an annual basis,
- divisions are required to adopt and maintain security controls, incident response protocols, and risk mitigation practices; and
- cybersecurity is evaluated as a core component of divisional asset protection, operational continuity, and insurance sustainability.

These expectations encompass networks, servers, endpoints, databases containing student and staff information, cloud-based learning platforms; and publicly accessible websites and portals.

Potential Impact of New Regulatory Standards under Bill 51

Bill 51 authorizes the creation of additional technical cybersecurity standards and mandatory programs, as well as incident reporting obligations to the minister or designate. While MSBA supports improved coordination and system-wide resilience, it cautions against:

- duplicative or conflicting standards;
- parallel reporting structures; and
- unfunded or under-resourced mandates.

Coherence with existing MSI cybersecurity standards is essential to:

- promote efficient use of limited financial and human resources;
- avoid compliance fragmentation; and
- ensure that funds directed toward cybersecurity actually reduce risk rather than administrative overhead.

Capacity Gaps and Implementation Realities

MSBA must emphasize that capacity gaps already exist within many school divisions, including:

- limited access to specialized cybersecurity professionals;
- competition with private sector wages;
- aging infrastructure in rural and northern communities; and
- increasing costs related to cyber insurance, threat monitoring, and remediation.

Any new regulatory obligations under Bill 51 must therefore be accompanied by:

- adequate, stable, and ongoing funding;
- realistic transition periods that allow for procurement, staffing, and training; and
- flexibility to accommodate divisions of varying size, geography, and technological maturity.

Consultation and Governance Considerations

Bill 51 recognizes the need for public consultation prior to most regulations and requires review of regulations within three years. MSBA strongly supports these provisions and stresses that:

- Consultation with MSBA must be explicit and continuous, given its role as advocate and particularly as the insurer for public school divisions;
- MSBA possesses deep, system-wide expertise regarding AI use in classrooms, cyber risk trends, strengths, vulnerabilities, and mitigation strategies; and
- school divisions are systems within a larger public-sector ecosystem, each with autonomous governance, statutory responsibilities, and operational realities.

Respect for this autonomy is fundamental to successful implementation.

Additional Observations and Recommendations

MSBA respectfully recommends that the Committee consider the following as Bill 51 advances:

1. **Education-First Approach**
   Regulatory frameworks should prioritize guidance, professional learning, and best-practice sharing rather than punitive or purely compliance-driven enforcement.
2. **Risk-Tiered Regulation**
   AI and cybersecurity requirements should be scaled according to risk, impact, and use context, particularly in instructional settings.
3. **Interoperability and Procurement Alignment**
   Regulations should support interoperable, standards-based procurement to prevent vendor lock-in and reduce long-term costs.
4. **Clarity on Ministerial Directives**
   Any authority to issue entity-specific cybersecurity directives should include safeguards,

transparency, and engagement with MSBA as insurer of public education in Manitoba and also with affected school boards, prior to issuance.

Conclusion

MSBA understands and supports Manitobans' desire for greater accountability in AI use and stronger cybersecurity protections across the public sector. Bill 51 is an important step in establishing a modern governance framework. For public education, both in terms of the academic and democratic dimensions of public education, its success will depend on respect for local governance and professional judgment; alignment with the existing, robust cybersecurity frameworks and requirements to which school divisions are already subject; adequate funding and transition time; protection of the overarching democratic structures, processes and institutions so critical to local democracy across Manitoba; and meaningful consultation with the Manitoba School Boards Association and especially with its members, who will be directly impacted by any new or emergent requirements under Regulation.

In summary then, what we want as MSBA on behalf of our members is flexibility and adaptability: please keep policy frameworks at a low/high level (low enough to remain adaptable and flexible but high enough to provide those in schools with enough direction or guidance to actually work with) because of the changing nature of AI; include guiding ethics with examples of beneficial use; establish resourcing and capacity for new school board members, administration and frontline staff in order to promote on-boarding of any new guidance, directives, or regulations, to protect divisional interests; and ensure that data protection and safeguards remain aligned with existing freedom of Information and privacy considerations (recognizing that large language models are not encrypted and so policies are needed to address disclosure), while also recognizing that any additional protections contemplated or yet to be developed under Bill 51 must respect human and academic freedom and the ability to use AI to promote its overall good and prospective benefits.

MSBA looks forward to continued collaboration with the Government of Manitoba to ensure that Bill 51 enhances student opportunity, system safety, local democracy, and long-term sustainability in Manitoba's public schools and across our communities. Public education is one of this province's greatest public goods. By working together to address and respond to Artificial Intelligence and Cybersecurity, we can work according to our common and unique strengths as elected officials in Manitoba– and avoid working at cross-purposes in future. If you wish to arrange a meeting with us to discuss these perspectives further, please do not hesitate to contact me at jwatt@mbschoolboards.ca. Thank you for your review of our observations and perspectives. We look forward to continuing our positive and collaborative relationship with you into the future.

Sincerely, and on behalf of our Provincial Executive and membership,

Josh Watt
Executive Director