Ontario introduces cyber and educational technology regulations

April 06, 2026

On March 23, 2026, the Ministry of Public and Business Service Delivery and Procurement published two regulations under the *Enhancing Digital Security and Trust Act, 2024* (EDSTA). O. Reg. 51/26 (Cyber Security) and O. Reg. 52/26 (Digital Technology Affecting Individuals Under Age 18) will both come into force on **July 1, 2026**. These regulations impose new governance, reporting, and transparency obligations on a broad range of Ontario public sector institutions, including universities, colleges, school boards, hospitals, and children's aid societies.

O. Reg. 51/26 – Cyber security

O. Reg. 51/26 applies to "prescribed public sector entities," which include colleges, universities, most public hospitals, school boards, children's aid societies, and other specifically named public sector entities.

Key updates

1. Cyber security maturity assessments: Prescribed public sector institutions must conduct cyber security maturity assessments at regular intervals, which track the institution's status or progress regarding cyber security. The regulation does not prescribe how the assessment must be performed, but states that it must be "carried out in accordance with industry standards or best practices endorsed by the Chief Information Security Officer of the Ministry".

First assessments must occur by July 1, 2027, and every two years thereafter. If an institution completes a cyber security maturity assessment between July 1, 2025, and July 1, 2026, the institution is deemed to have completed it on July 1, 2026, and must complete its second assessment by July 1, 2028.

A summary of each assessment must be provided to the Ministry within 30 days of completion, which must include (1) the name and a description of the model or framework used in the assessment, (2) any overall or component cyber security maturity score, and (3) a summary of areas for future improvement.

2. Point of contact: The regulation requires each prescribed public sector entity to designate a senior management employee as the primary cyber security point of contact. This individual must have decision making authority over cyber security and will be responsible for liaising with the Ministry and approving summaries of cyber security maturity assessments. For many institutions, this will require a governance conversation: the role may be assigned to a CIO, CISO, or another executive.

3. Incident reporting: Prescribed public sector institutions must also report "critical cyber security incidents" to the Ministry within 72 hours of "confirming" the incident occurred. "Critical cyber security incident" is defined broadly and includes incidents that impact "digital information" collected, used, retained, or disclosed by an institution or the infrastructure housing or transmitting such data. It also includes a materiality threshold. To meet the reporting threshold, one of the following criteria must be satisfied:

- The incident results in a significant adverse impact to the delivery of public services by the entity;
- The incident poses a risk to public safety;
- The incident requires or results in significant efforts to recover digital information or related infrastructure or activation of cyber security incident response plans by the entity; or
- The incident poses a significant risk of harm to the reputation of and public confidence in the entity.

The "confirmation" requirement and materiality threshold ought to rule out cyber events and low severity incidents, though compliance with the reporting requirement is an important consideration that institutions should build into their incident response plans. Bearing mind that "activation of a cyber security incident response plans" triggers a reporting duty, institutions should also ensure their plans clearly define an activation point.

What does O. Reg. 51/26 mean for public sector institutions?

O. Reg. 51/26 encourages enhanced cyber security by requiring institutions to perform maturity assessments and report such assessments to the province. Cyber incident reporting already occurs informally today, but formal reporting will come with important confidentiality protections that the province has proposed in bills amending the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Privacy Act* (MFIPPA). See our companion article: Major access and privacy reform comes to Ontario.

The province will receive reports not as an enforcement body, but as a provider of security funding and as a potential agent for cross-institutional, province wide collaboration. There is therefore reason for institutions to view these new obligations positively, though cyber incident reporting must not invite heavy post-reporting obligations that draw critical resources away from the response. Institutions must be prepared to manage this potential for disruption.

O. Reg. 52/26 – Digital technology affecting individuals under age 18

O. Reg. 52/26 applies to all school boards in Ontario and applies to all personal information in digital form of students under the age of 18.

Key requirements

The regulation prescribes certain notice requirements relating to disclosures of student personal information to a board's software providers. Notices must be in writing and can be delivered electronically. For students under the age of 16, notices must be sent to parents. For students between the ages of 16 and 18, notices must be sent to the students. The notice must include:

- The specific personal information being disclosed;
- The legal authority for the disclosure;
- The purpose of the disclosure;
- The name of the application and vendor;
- Contact information for a Board representative who can answer questions about the disclosure; and
- An explanation of complaint and oversight rights.

Boards will be required to provide the notice as early as feasible in the school year. If new software is implemented during the school year, notice of disclosure must be provided as soon as feasible.

What does O. Reg. 52/26 mean for public sector institutions?

The regulation reflects growing concern about educational technology platforms and their data practices, particularly where third party vendors are involved. Boards should anticipate and be prepared for parental scrutiny. Conducting privacy impact assessments that comply with the requirements that will soon be set out in MFIPPA will help.

In addition to developing a plan to formally implement an MIFPPA-compliant privacy impact assessment program, boards will need to ensure that they have a complete inventory of all software used by a board and the personal information disclosed to each software provider by September 2026. This mapping task is a priority.

Conclusion

These regulations are an incremental update to Ontario privacy and data security law. They meaningfully change how public institutions are expected to manage cyber security and, particularly in the education sector, how they deploy and oversee digital tools affecting children.

Taken together, O. Reg. 51/26 and O. Reg. 52/26 is another indication that Government and regulators expect demonstrable accountability for public sector digital governance, privacy, and cybersecurity.

For additional questions, please reach out to one of the key contacts listed below.

By

Daniel J. Michaluk, Marc Vani, Avital Sternin

Expertise

Cybersecurity, Privacy & Data Protection, Health Law, Education

---

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 800 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

The information contained herein is of a general nature and is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser in cases of specific questions or concerns. BLG does not warrant or guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP. If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to remove your contact information from our mailing lists by emailing unsubscribe@blg.com or manage your subscription preferences at blg.com/MyPreferences. If you feel you have received this message in error please contact communications@blg.com. BLG's privacy policy for publications may be found at blg.com/en/privacy.

© 2026 Borden Ladner Gervais LLP. Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.