February 9, 2026

OPSBA Submission re: Proposed Regulatory Requirements under the *Enhancing Digital Security and Trust Act* – Cyber Security

The Ontario Public School Boards' Association (OPSBA) appreciates the opportunity to provide comments and feedback to the current proposal initiated by the Ministry of Public and Business Service Delivery and Procurement (MPBSDP) and the new regulations under *the Enhancing Digital Security and Trust Act*, 2024 pertaining to cyber security.

We are supportive of the new requirements for school boards to implement cyber security programs and to provide notice when students' personal information is disclosed to third party owners or operators of software applications. However, school boards will need to be supported to fulfil these requirements as directed.

This need to fully support and address cyber security issues was included in our recent funding submission in which we reminded the Standing Committee on Finance and Economic Affairs that, "*School boards are increasingly targeted by cyber-criminals due to the volume of sensitive data under their control, the number of board users with access to this data, and inadequate dedicated funding to support strong cyber security environments in school boards. Without targeted dedicated cyber security funding, school boards face increasing likelihood of service disruption, financial losses, legal exposure, and compromised student and staff data*."

Like many other public entities, school boards have been victims of cyber attacks. Many boards across the province were affected by the PowerSchool cyber-security incident in late 2024 and early 2025 that involved the unauthorized external access of student personal information and private records. The sector worked with the Ontario School Boards' Insurance Exchange (OSBIE) in the development of some resources and capacity building.

Last year's Core Education Funding included a one-time small amount of funding to boards to implement foundational security tools. However, there continues to be a need for consistent and dedicated funding for boards to reduce the high risks and address the increasing costs associated with cyber security. Thes costs include staffing, professional development, and resources. Beyond the technical risks to infrastructure, the ministry must address the human dimension of cyber security, specifically the evolving threats students face on platforms like Roblox, Discord, and Minecraft. To manage these risks effectively, dedicated funding is essential to provide continuous professional development for school-based staff.

OPSBA is aware of a current one year pilot program involving 23 school boards and the Education Collaborative Network of Ontario to provide funding for a Security Operations Centre (SOC.) The SOC is to be staffed by a third party entity and provide a 24/7 security centre for these boards to handle and deal with cyber threats and potential risks. We are hopeful that this pilot program will highlight the real needs of the education sector but are concerned that this this initiative is in place for only one year. We would ask that the information and data collected from this pilot program be shared with the sector.

The safety and security of student and staff information is a priority for OPSBA and its member boards and we want to ensure this is addressed by the Ministry of Education.

Regarding the draft regulation and the consultation questions, OPSBA's Policy Development Work Group had the following questions and concerns:

- Core Education Funding must address the critical need and increasing costs of cyber security – will there be dedicated funding including in the next grant provision?
- The proposed regulation requires one primary cyber security contact and one alternate at each school board. Will there be funding to support this responsibility and the additional work?
- Will the Cyber Security Maturity Assessments include a checklist for boards? (security projects/initiatives, backup and recovery plans, communication plans to stakeholders, etc.)
- It is not clear how many boards are aware of the Cyber Security Ontario Portal and its resources. How was this information shared and communicated?
- Is there any tie to Supply Ontario and procurement of licences that would be of benefit to boards?
- It is important to note and understand the differences among school boards. Some may have a Chief Information Officer or an Information Technology Manager, but many do not. There are variances in the sophistication and comprehensiveness of IT departments and the skill level and number of qualified staff (internal capacity and resources).

OPSBA will continue to share information and work with the Ministry of Education on this very important issue. Given the rapidly evolving threat landscape, it is imperative that the government and school boards remain agile. Our Association is committed to a continuous partnership with the ministry to ensure our defenses and funding models keep pace with emerging digital risks, and that student, staff and parent/caregiver information remains secure. The mitigation of risk needs to be a top priority.

,

The Ontario Public School Boards' Association represents English public district school boards and public school authorities across Ontario, which together serve nearly 1.4 million public elementary and secondary students. The Association advocates on behalf of the best interests and needs of the public school system in Ontario. OPSBA is seen as the credible voice of public education in Ontario and is routinely called on by the provincial government for input and advice on legislation and the impact of government policy directions.