The PowerSchool IPC report: Five tips for school boards and Ontario institutions

November 27, 2025

On November 17, 2025, the Ontario Information and Privacy Commissioner (IPC) released a complaint report arising from the December 2024 cyberattack against the PowerSchool Student Information System (SIS). The report is the IPC's most current guidance on the obligations of Ontario public sector institutions that outsource systems for processing personal information.

The findings

Twenty public school boards reported the PowerSchool incident to the IPC.

A threat actor used compromised credentials with elevated permissions to access multiple SIS environments and exfiltrated data relating to current and former students, parents/guardians, and educators.

The IPC concluded that, as a whole, the institutions did not have reasonable measures in place to prevent unauthorized access. It focused on the respondent boards' management of PowerSchool, stressing the need for school boards to collaborate in obtaining more protective contractual terms and the need for school boards to proactively administer their relationship with PowerSchool to better protect student information.

Implications of the report

For the past fifteen years, school boards and other Ontario institutions in the public sector have outsourced many IT services, leaving student, employee and other personal information to be protected by vendors. The PowerSchool incident and the IPC report underscore the due diligence required of institutions who adopt this service delivery model. Outsourcing can save internal costs and improve security, but it also can invite a range of risks associated with lessened control. And the IPC has now made clear that it expects a strong form of due diligence to be applied in contracting with vendors and overseeing their performance.

Tips for school boards and Ontario institutions

Here are our five practical tips.

Tip 1 - Consider risk in deciding whether to outsource

Before outsourcing critical IT services, weigh the potential benefits against the risks of diminished control over sensitive data. There is a basic level of risk to consider in deciding whether to outsource at all, particularly when there are few vendors to select from.

Also, the IPC report underscores that outsourcing does not absolve boards of accountability, and that the activities associated with diligently managing vendors require resourcing. Consider whether you have the resources to manage the proposed outsourcing.

Tip 2 - Negotiate for compliance

The IPC expects institutions to attempt to secure appropriate protective clauses that enable proactive oversight and enforceable accountability that are generally aligned with its 2024 outsourcing guidance - *Privacy and Access in Public Sector Contracting with Third Party Service Providers*. It has encouraged institutions to collaborate through joint procurement initiatives.

It may not be possible to obtain contract terms that are fully aligned with the IPC's expectations, but engaging in a *bona fide* negotiation of data protection terms is a means of demonstrating due diligence. Gaps between ideal terms and what can be obtained may result from negotiation. It may still be reasonable to proceed with an outsourcing despite such gaps; less than optimal data protection terms are a matter of risk that institutions should identify, assess and mitigate through appropriate action.

Tip 3 - Have a vendor management policy

Internal responsibility for vendor oversight should be clearly defined. Institutions should designate specific individuals to be responsible for managing the contracting process and vendor compliance and performance. Clear accountability within an institution helps ensure that risks are identified early and mitigated effectively, aligning with the IPC's emphasis on proactive and ongoing contract administration.

Tip 4 - Apply demonstrable accountability

The IPC has recently raised the importance of demonstrable accountability: "a repeatable and demonstrable system of data governance whereby organizations can show regulators more concretely, backed by evidence, how they meet their legal requirements in practice." Institutions must be able to show – not just claim – that they have exercised due diligence. This means maintaining records of vendor risk assessments, contract negotiations, and ongoing monitoring activities.

Tip 5 - Develop an exit strategy

Institutions should have a clear plan for termination of outsourced services and for data transition to a new service provider. An exit strategy ensures that, if a vendor fails to

meet obligations or experiences a breach, institutions can disengage without facing service disruption problems and without compromising data integrity. Continuity planning is a critical component of vendor risk management.

Conclusion

While the IPC's PowerSchool report does not introduce new principles, it strongly reinforces an idea that has been stressed by the IPC for years: accountability in outsourcing is essential to meeting statutory obligations. Attempting to negotiate protective terms is required despite the potential for vendor resistance, and once a contract is settled and services initiated, there remains an ongoing oversight duty.

BLG is a leading advisor to the Ontario school board and broader public sector on IT contract negotiations and privacy and security compliance and risk management. Please reach out to us for assistance in meeting your obligations.

By

Daniel J. Michaluk, Shane Morganstein, Krystin Chung

Expertise

Cybersecurity, Privacy & Data Protection, Information Technology, Education

---