Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINTS MR25-00002, MR25-00003, MR25-00004, MR25-00005, MR25-00006, MR25-00007, MR25-00008, MR25-00009, MR25-00010, MR25-00011, MR25-00013, MR25-00014, MR25-00015, MR25-00016, MR25-00017, MR25-00018, MR25-00019, MR25-00020, MR25-00021, MR25-00026, PR25-00002

Toronto District School Board, Peel District School Board, Thunder Bay Catholic District School Board, Lakehead District School Board, York Region District School Board, Brant Haldimand Norfolk Catholic District School Board, Near North District School Board, Northwest Catholic District School Board, Northeastern Catholic District School Board, Rainy River District School Board, Keewatin-Patricia District School Board, Superior North Catholic District School Board, Durham District School Board, Dufferin-Peel Catholic District School Board, London District Catholic School Board, Wellington Catholic District School Board, Halton Catholic District School Board, Simcoe Muskoka Catholic District School Board, Ottawa Catholic School Board, Superior-Greenstone District School Board, and the Ministry of Education

November 17, 2025

TABLE OF CONTENTS

Summary: Twenty school boards and the Ministry of Education (collectively, the institutions) each reported to the Information and Privacy Commissioner of Ontario they were victims of a cyberattack against their third-party service provider, PowerSchool Canada ULC (PowerSchool). A threat actor gained access to PowerSchool's student information system (SIS) and customer support portal, PowerSource via compromised credentials and exfiltrated personal data held in the SIS. The personal data included the personal information of current and former students, their parents or guardians, and current and former staff. The cyberattack was discovered when PowerSchool received a ransom demand from the threat actor. The institutions notified the affected individuals about the cyberattack. PowerSchool hired experts to investigate the cyberattack but was unable to determine how the threat actor gained access to compromised credentials.

In this report, I conclude that the institutions did not have reasonable measures in place to prevent unauthorized access to the personal information in their custody or control, as required by section 3 of Regulation 823 under *MFIPPA* and section 4 of Regulation 460 under *FIPPA.* I find there were shortcomings in certain institutions' Agreements with PowerSchool that lacked reasonable provisions to ensure the privacy and security of the personal information held by PowerSchool on behalf of the institutions. Moreover, institutions lacked the necessary oversight measures to effectively and regularly monitor PowerSchool's fulfillment of its contractual obligations.

In some cases, institutions over-collected sensitive personal information and retained personal information far longer than necessary by not implementing appropriate retention schedules and not regularly purging personal information accordingly. This had the effect of exposing massive volumes of personal data to the threat actor and amplifying the real risk of significant harm to those individuals impacted. I also conclude the institutions did not, as a whole, respond adequately to the breach because of inadequate or a complete lack of privacy breach response plans, protocols and/or policies.

In light of my findings, I recommend that the institutions take remedial actions including as follows: limit PowerSchool's remote maintenance support access to an as-needed basis only; strengthen their early breach detection process and privacy breach response plans; cease any unnecessary collection of personal information and only retain personal information as long as necessary to avoid amplifying the risk of harm when a breach occurs. I further recommend that institutions implement privacy impact assessments to evaluate the privacy implications of the technologies they use or are considering adopting, including through service providers, such as PowerSchool and that they exercise due diligence throughout the procurement process from planning to decommissioning.

I recommend that the institutions, as they review and renegotiate their Agreements with PowerSchool, as needed, to ensure reasonable contractual provisions are in place to protect privacy and security of personal information in their custody or control. I also recommend that the institutions improve their oversight measures in respect of PowerSchool by reviewing PowerSchool's security and information management policies to ensure compliance with the Agreements, including insisting on receiving copies of annual security audit reports, certifications and risk assessments. Finally, I recommend that the institutions include sufficiently robust enforcement provisions in their Agreements with PowerSchool and take decisive action to exercise these provisions to ensure PowerSchool takes prompt and necessary measures to provide

documents on request and remediate any non-compliance found with respect to their contractual obligations.

Statutes Considered: *Freedom of Information and Protection of Privacy Act,* R.S.O. 1990, c. F. 31 , (*FIPPA*); R.R.O. 1990, Reg. 460 (Regulation 460); *Municipal Freedom of Information and Protection of Privacy Act* , R.S.O. 1990, c. M. 56 ; R.R.O. 1990, Reg. 823 (Regulation 823); and *Education Act*, R.S.O. 1990, c. E.2.

Investigation Reports Considered: Privacy Complaint Reports MC18-48, MC17-52, PR16-40, and Special Investigation Report PC12-39.

BACKGROUND:

[1] In January 2025, 20 Ontario school boards (boards) and the Ontario Ministry of Education (ministry), (collectively, the institutions), independently reported a breach[1] of personal information to the Information and Privacy Commissioner of Ontario (IPC). The breach involved a cyberattack on the institutions' Student Information System (SIS) and the customer support portal, PowerSource, through their third-party service provider, PowerSchool Canada ULC (PowerSchool).

[2] The following boards reported the cyberattack to the IPC:

- Toronto District School Board;
- Peel District School Board;
- Thunder Bay Catholic District School Board;
- Lakehead District School Board;
- York Region District School Board;
- Brant Haldimand Norfolk Catholic District School Board;
- Near North District School Board;
- The Northwest Catholic District School Board;
- Northeastern Catholic District School Board;
- Rainy River District School Board;
- Keewatin-Patricia District School Board;

[1] Although it was not statutorily mandated at the time of this breach, as of July 1, 2025, institutions subject to *FIPPA* are required to report a privacy breach to the IPC.

- Superior North Catholic District School Board;
- Durham District School Board;
- Dufferin-Peel Catholic District School Board;
- London District Catholic School Board;
- Wellington Catholic District School Board;
- Halton Catholic District School Board;
- Simcoe Muskoka Catholic District School Board;
- Ottawa Catholic School Board; and
- Superior-Greenstone District School Board.

[3] The above-noted boards govern all schools within their respective jurisdictions that provide education services to students in English and French public and Catholic elementary and secondary schools.[2]

[4] Additionally, the ministry reported to the IPC on behalf of the Provincial and Demonstration Schools Branch, responsible for operating English and/or American Sign Language Provincial schools and Demonstration schools. These schools provide education programming for visually or hearing-impaired children and children with severe learning disabilities.

[5] The above-listed boards and the ministry are obligated to prevent unauthorized access to personal information in their custody or control under the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA)* and the *Freedom of Information and Protection of Privacy Act* (*FIPPA),* respectively (collectively, the *Acts*). While service providers like PowerSchool are not subject to the *Acts*, I acknowledge that PowerSchool voluntarily notified this office of the cyberattack on January 27, 2025.

[6] The IPC also received 12 complaints from parents, guardians, a teacher and former students about the cyberattack. The personal information of approximately 3.86 million Ontarians was affected by the cyberattack.

[7] Considering the magnitude of the cyberattack and the sensitivity of the personal information of children and youth, the matter moved to the formal Investigation Stage of the IPC's complaint process.

[8] As part of my investigation, I requested and received written representations from the institutions, which included some information provided to them by PowerSchool. To

[2] Education facts | ontario.ca

address confidentiality and security concerns, I have only included information that is necessary for this report and in some cases have generalized information from the confidential representations provided.

PowerSchool's Education-Based Information Management System and Portal

[9] In order to store and manage data related to students and educators[3] from Kindergarten to Grade 12 (K-12), the institutions[4] use a third-party education-based information management system called PowerSchool SIS,[5] owned and operated by PowerSchool. The institutions independently retained PowerSchool under their respective contractual agreements (the Agreements) to provide data management services related to registration, attendance tracking, scheduling, provincial compliance reporting, staff data management, and management of emergency, medical and health information to assist the institutions in meeting their obligations under the Ontario *Education Act.*[6] Each institution has its own designated SIS environment where the personal information relating to the institution's operations is stored. An institution may configure its SIS environment to provide access to students, their parents, guardians, teachers and educational administrators. At issue in this report was the personal information held within these SIS environments.

[10] PowerSchool's SIS is integrated with other PowerSchool education-based technologies, one of which is PowerSource. It is an umbrella portal that is also interconnected with all of PowerSchool's products, including SIS.[7]

[11] At the time of the cyberattack, PowerSource was accessible to certain authorized users (institutions' staff members including teachers, administrators and information technology staff) who could download technical support information relating to the institution's SIS environment. Further, certain authorized PowerSchool employees or contractors could access an institution's SIS, with the institution's consent, for technological maintenance purposes or to resolve support requests from the institution.

The Cyberattack

[12] According to information provided to the IPC, the cyberattack and events following the cyberattack occurred as follows.

[13] On December 28, 2024, PowerSchool became aware that a threat actor had gained access to various SIS environments through PowerSource using the credentials of a subcontractor who worked for PowerSchool to perform technical support. During the

---

[3] The term educators encompasses different individuals from each institution, such as principals, vice-principals, teachers, classroom support staff, office staff, guidance counsellors, superintendents, and administrative liaisons, among others.
[4] In this matter, the institutions are "customers" of PowerSchool.
[5] SIS is used by many Canadian and international schools or school districts. See: PowerSchool SIS.
[6] R.S.O. 1990, c. E.2 (*Education Act*).
[7] PowerSource.

course of the IPC's investigation, PowerSchool first referred to this individual as a former contractor, then in later representations, referred to them as a "former subcontractor" working with PowerSchool.

[14] Only when the IPC shared a draft version of this report with PowerSchool which referred to a "former subcontractor", did PowerSchool advise that the contractual relationship with the subcontractor concluded in January 2025, after the cyberattack, and therefore that the subcontractor was actively working during the cyberattack. PowerSchool stated that its reference to the term "former" reflected the subcontractor's status as of the date(s) PowerSchool provided its responses to the IPC and that "it was not to suggest the subcontractor was "former" at the time of the incident".

[15] This report is based on PowerSchool's late assertion that the subcontractor was active at the time of the cyberattack, although I cannot make a factual finding that this assertion is true. In my view, there is a very clear and important distinction between a contractor and a subcontractor and understanding their status at the time of a breach incident is critical.[8]

[16] Upon discovery of the cyberattack, PowerSchool initiated its cybersecurity incident response protocol and organized a cross-functional response team, including third-party cybersecurity experts, to contain the threat and determine the scope of the cyberattack.

[17] On January 7, 2025, PowerSchool informed the institutions that it had experienced a cyberattack, but that the matter was contained. Over the following days, the institutions activated their own privacy breach response plans or protocols and engaged with their third-party breach experts and/or legal counsel to determine the scope of impact. The institutions confirmed their internal networks and servers (other than their SIS environments) were not impacted by the cyberattack.

[18] Through their third-party breach expert's investigation, PowerSchool learned the threat actor used the compromised account of a subcontractor to set up an automated script[9] to copy and exfiltrate two database tables: the student table and the educator table which contained information from each institution's respective SIS.

[19] According to PowerSchool, it was not locked out of its SIS or PowerSource and there was no evidence of malicious encryption, malware or further unauthorized activity at the time of the cyberattack. PowerSchool and the institutions did not experience any operational disruptions to their systems or networks.

---

[8] According to PowerSchool's internal ISMS Governance Policy, a sub-contractor is defined as "a person or organization contracted by another third-party to deliver tools or services for PowerSchool…Use of sub-contractors is prohibited unless specifically approved in the vendor's master services agreement (MSA) or statement of work (SOW)".

[9] An automated script is defined as a list of digital instructions that execute commands such as data transfer. See: Automated Process - Glossary | NIST.

[20] Approximately 5.2 million Canadians living across several provinces and territories were impacted by the cyberattack on PowerSchool's SIS and PowerSource. In addition to the IPC's investigation, other Canadian Information and Privacy Commissioners are investigating or have investigated[10] the public institutions affected in their respective jurisdictions in accordance with their applicable provincial or territorial privacy legislation. In addition, the Office of the Privacy Commissioner of Canada (OPC) investigated PowerSchool's role in this matter under the federal *Personal Information Protection and Electronic Documents Act*[11] (*PIPEDA*). The OPC investigation resulted in a voluntary Letter of Commitment entered into by the OPC and PowerSchool.[12]

[21] The information at issue in this investigation relates to the compromised personal information of affected Ontarians, which includes current and former students; their parents or guardians; and current and former educators at the institutions.

Ransom Demands and Payment

[22] According to information provided by certain institutions and PowerSchool, the threat actor sent their initial ransom demand by email to PowerSchool on December 28, 2024. Despite the fact that PowerSchool paid the ransom in or around January 2025, the threat actor sent another email on May 4, 2025, to the Toronto District School Board (TDSB) and Peel District School Board (PDSB), among others, demanding ransom payment to prevent release of the same data at issue. The IPC was informed of this new extortion attempt on May 5, 2025 by TDSB and on May 7, 2025 by PDSB.

[23] On May 7, 2025, PowerSchool informed the IPC that it became aware of these new extortion attempts. PowerSchool did not believe it was a new cyberattack and advised the IPC that it was actively monitoring and addressing the matter including working with law enforcement and that a public statement from PowerSchool would be issued.

[24] On the same day, PowerSchool publicly stated, "in the days following our discovery of the December 2024 incident, we made the decision to pay a ransom because we believed it to be in the best interest of our customers and the students and communities we serve.[…]. As is always the case with these situations, there was a risk that the bad actors would not delete the data they stole, despite assurances and evidence that were provided to us".[13]

---

[10] See the Office of the Saskatchewan Information and Privacy Commissioner's Investigation Report: 003-2025, 035-2025.
[11] S.C. 2000, c. 5 (*PIPEDA*).
[12] News release: PowerSchool commits to strengthened breach measures following engagement with the OPC.
[13] See PowerSchool's May 7, 2025 Notice: SIS Incident | PowerSchool.

[25] Contemporaneously, TDSB[14] and PDSB[15] issued public statements describing developments related to the second ransom demand involving the same data that was at issue in the December 2024 cyberattack. In their respective statements, TDSB and PDSB advised they were working closely with PowerSchool, law enforcement and the IPC. TDSB also issued direct notices to current students, their parents or guardians and current educators.

[26] Following communications with a threat actor group, PowerSchool says it was shown a video of the data at issue being deleted using a secure deletion software and the threat actor group reiterated its agreement not to publish the data at issue. During this communication, PowerSchool also learned that a member of the threat actor group had gone rogue and made the second ransom demand to TDSB and PDSB, among others.

[27] The harsh reality in the digital world is that once data is stolen, it is beyond the institutions' and service provider's control with no guarantee of successful containment. In my view, unless institutions have clear and unequivocal evidence showing otherwise, they should not rely on a threat actor's "promises", rather, they should assume that the threat actor is using, or may still use, the stolen data in the future.

[28] To date, there has been no evidence of publication or sale of the compromised data on the dark web. If future monitoring reveals that this has happened, I recommend the institutions re-notify the IPC as soon as feasible.

Criminal Sentencing of a 19-Year-Old Student

[29] According to a Press Release[16] issued by the United States (US) Attorney's Office for the District of Massachusetts on May 20, 2025, a 19-year-old student was charged[17] with cyber extortion crimes, among other charges. The student, formerly a member of the threat actor group, agreed to plead guilty[18] to hacking two US-based companies' computer networks (one being PowerSchool[19]) and extorting the companies for ransoms. The student had demanded approximately 2.85 million (30 Bitcoin) in US dollars as ransom at the time to stop him from leaking more than 60 million students[20] and 10

---

[14] See TDSB's May 7, 2025 Notice: News: Letter to Parents, Guardians and Caregivers re: 2024 Power School Cyber Incident | TDSB.
[15] See PDSB's May 7, 2025 Notice: Families Update: 2024 Power School Cyber Incident - PDSB.
[16] District of Massachusetts | Worcester College Student to Plead Guilty to Cyber Extortions | United States Department of Justice.
[17] US v. Matthew Lane - Information.
[18] US v. Matthew Lane - Plea Agreement.
[19] I note that PowerSchool is not publicly named as a victim in the Press Release or associated court documents. However, several USA and Canadian media outlets indicate on October 15, 2025, PowerSchool confirmed that the student was the individual behind the cyberattack. See: Man behind PowerSchool breach that exposed Canadian students' data sentenced to 4 years in prison | CBC News.
[20] At the time of the cyberattack, PowerSchool's website stated it connects "60 million+ students" around the world which appears to be consistent with the facts set in the above noted Press Release and associated court documents. See: PowerSchool K-12 Software & Cloud-Based Solutions.

million teachers' data.[21]

[30] On October 14, 2025, the student was sentenced[22] to four years in prison and was found guilty of cyber extortion conspiracy, cyber extortion and unauthorized access to protected computers by a US District Judge in Worcester, Massachusetts.

PRELIMINARY ISSUES:

[31] There is no dispute that the boards and the ministry are "institutions" under section 2(1) of the *Acts*. PowerSchool is a "service provider" as defined in the *IPC Guidance: Privacy and Access in Public Sector Contracting with Third Party Services Providers*.[23] PowerSchool delivers services to the institutions using an information management system and portal to assist the institutions with managing their education-based information.

[32] Further, there is no dispute that the information at issue includes "personal information"[24] as defined under section 2(1) of the *Acts.* It is also not disputed that the collection of the affected personal information by the threat actor(s)' was not "expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity" under sections 28(2) of *MFIPPA* and 38(2) of *FIPPA*. It is also clear that the access to, and exfiltration of, this personal information by the threat actor, who was not an agent of the institutions or acting on their behalf, constitute an unauthorized use and unauthorized disclosure of personal information under the *Acts*.

ISSUES:

1. Did the institutions have reasonable measures in place to prevent unauthorized access to personal information in accordance with the requirements of the *Acts* and their regulations?

2. Did the institutions, as a whole, respond adequately to the breach?

INVESTIGATION:

[33] During my investigation, I made multiple requests from each institution. The institutions advised that most of the relevant information I was seeking was in

---

[21] See para. 14: US v. Matthew Lane - Information.
[22] #22 in United States v. Lane (D. Mass., 4:25-cr-40015) – CourtListener.com; #21 in United States v. Lane (D. Mass., 4:25-cr-40015) – CourtListener.com; #20 in United States v. Lane (D. Mass., 4:25-cr-40015) – CourtListener.com.
[23] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.
[24] Fact Sheet: What is Personal Information? | IPC.

PowerSchool's possession, requiring coordination among these entities. At the outset, PowerSchool voluntarily provided the IPC with some of this information.

[34] As I pursued my investigation, I noted many inconsistencies in the responses received from institutions and PowerSchool. Specifically, I found certain information in their submissions contradicted publicly available information on their respective websites. Further, in their responses to my questions, many institutions only cited broad data and privacy commitments from PowerSchool's website[25] and provisions from a cybersecurity industry standard manual.

[35] As I persisted in my requests for further information, most institutions made additional attempts to obtain responsive information from PowerSchool. However, many of them reported back that they had received incomplete information from PowerSchool. Further, most institutions advised the IPC that PowerSchool had been hesitant to provide them with any information, taking the position that PowerSchool first needed assurances from the IPC and the institutions that sensitive information will remain confidential.

[36] Despite PowerSchool not being a regulated entity under the *Acts*, given the above, the IPC decided to also directly engage with PowerSchool. The IPC assured PowerSchool that this office does not publish confidential and sensitive information in its decisions, where the disclosure of that information may pose a security risk to an organization.

[37] Based on this assurance, PowerSchool subsequently provided the IPC with additional information. As indicated earlier in this report, I have only included information necessary for this report and in some cases, I have generalized information received to avoid compromising PowerSchool's or the institutions' security postures.

[38] In this report, I make recommendations that apply to all or some of the institutions without naming specific institutions. I also comment on some of PowerSchool's security safeguards to the extent these are relevant to whether the institutions implemented reasonable contractual and oversight measures over their service provider to ensure the institutions' own compliance with the *Acts* and their regulations.

DISCUSSION:

Issue 1: Did the institutions have reasonable measures in place to prevent unauthorized access to personal information in accordance with the requirements of the *Acts* and their regulations?

[39] Section 3 of Regulation 823 of *MFIPPA* states:

> (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined,

[25] I note PowerSchool updated information on its website since the cyberattack.

> documented and put in place, taking into account the nature of the records to be protected.
>
> (2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.
>
> (3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

[40] Section 4 of Regulation 460 of *FIPPA* contains identical language.

[41] The boards must comply with section 3 of Regulation 823 of *MFIPPA*, while the ministry must comply with section 4 of Regulation 460 of *FIPPA*.

[42] The *Acts* and their regulations do not prescribe the specific measures that must be taken to protect personal information and there is no one-size fits all approach. What are "reasonable measures" will depend on the nature of the records to be protected, including their sensitivity, the level of risk, and the types of threats posed to them.[26]

[43] Moreover, while institutions may outsource some of their responsibilities to third party service providers, they remain ultimately accountable for ensuring reasonable measures are in place to prevent unauthorized access to personal information under their custody or control.

A. Technical and Security Safeguards

[44] To assess the technical and security safeguards in place at the time of the cyberattack, I reviewed a number of documents as part of my investigation.

[45] PowerSchool provided the IPC with a copy of its February 28, 2025 Investigation Report[27] into the cyberattack prepared by a third-party cybersecurity expert.

[46] The institutions and PowerSchool further provided me with the following documents related to PowerSchool's SIS and PowerSource privacy and security measures at the time of the cyberattack:

- Information Security Management System Governance Policy (ISMS Governance Policy);
- System and Organization Controls 2 Type 2 Report (SOC 2 Type 2 Audit Report);

[26] See para. 72 of Privacy Complaint Report PR16-40.
[27] See PowerSchool Investigation Report Final, which PowerSchool provided to the IPC on March 4, 2025.

- ISO 27001:2022 First Surveillance Audit Report (ISO Standard Surveillance Audit Report);
- Penetration Testing Summary Report;
- Network Security Diagram;
- PowerSchool Memos; and
- Security Incident Response Procedure.

[47] PowerSchool's ISMS Governance Policy describes the established operational security controls that apply to all PowerSchool employees and contractors while using PowerSchool's information assets. This ISMS Governance Policy encompasses various PowerSchool policies (Access Control Policy, Third Party Management Policy, Asset Management Policy, Password Policy, Incident Response Policy, Monitoring Policy, Security Awareness & Training Policy, among others) which are discussed individually throughout this report.

[48] Based on the available facts, and my analysis below, I conclude that a number of vulnerabilities contributed to a threat actor successfully exploiting PowerSchool's SIS and PowerSource, including the following: compromised credentials of an elevated user, the lack of MFA required for PowerSchool users to access PowerSource (through which SIS can be accessed), the "always on" feature for remote maintenance support, and the failure to detect and respond to the earlier unauthorized activities in a timely manner due in part to the limited log retention period.

i. User Privileges

[49] According to PowerSchool, the root cause of this cyberattack was due to the threat actor's ability to use compromised credentials belonging to a subcontractor[28] who worked remotely in a technical support role based outside the USA at the time of the cyberattack. The subcontractor had elevated privileges to access PowerSource and through it, the institutions' individual SIS environments where institutions had enabled remote maintenance support[29] connections by selecting the "always on" option. This option allowed the threat actor to gain access into the institutions' SIS environments through PowerSource. The subcontractor's elevated privileges were high enough to allow a threat actor to conduct a vast amount of unauthorized activity.

[50] PowerSchool's experts were unable to determine how the threat actor gained initial access to the compromised credentials, and at the time of writing this report,

[28] According to PowerSchool's internal ISMS Governance Policy, a sub-contractor is defined as "a person or organization contracted by another third-party to deliver tools or services for PowerSchool…Use of sub-contractors is prohibited unless specifically approved in the vendor's master services agreement (MSA) or statement of work (SOW)".

[29] PowerSchool Investigation Report Final.

PowerSchool's investigation into this matter is still ongoing.[30]

[51] In my view, it is concerning that the same compromised credentials were used by an unknown threat actor to enter PowerSource, potentially multiple times between August 16, 2024 and September 17, 2024, then ultimately in December 2024.[31]

[52] Given the somewhat vague responses from PowerSchool about the subcontractor's compromised credentials at the time of the cyberattack, I recommend the institutions review PowerSchool's ISMS Governance Policy to confirm it meets the relevant industry standards that are reasonable in the circumstances.

[53] For example, the National Institute of Standards and Technology (NIST) sets out access control and privilege guidelines recommending specific maintenance personnel policies and procedures to be implemented within systems and organizations. The guidelines recommend strong authentication requirements for remote maintenance personnel who are based outside the USA, which was the case of the subcontractor here.[32]

[54] Institutions should confirm that PowerSchool's ISMS Governance Policy addresses subcontractors' access privileges to ensure user access privileges are granted, modified and revoked within a reasonable time period based on employment status and job requirements. In addition, the institutions should review the policy to require reasonable logging of actions associated with particular credentials. Failure to do so can render an organization more vulnerable to cyberattacks such as this.

[55] I recommend the institutions demand PowerSchool make changes to its ISMS Governance Policy, where the institutions deem it necessary to address elevated access privileges for remote personnel, and monitor implementation of those changes. I also recommend that the institutions demand that PowerSchool adopt the least privilege principle. This would help ensure that a PowerSchool employee, agent, contractor or subcontractor who is given access to PowerSource to fulfill their role and responsibilities, is provided with only the minimum privileges necessary to do so, and for only as long as authorized by the institution and PowerSchool.

B. Passwords and Multi-Factor Authentication

[56] When I asked for details on the complexity and length requirements for PowerSchool's passwords and the use of multi-factor authentication (MFA)[33] to access

---

[30] The IPC was not provided additional evidence relating to PowerSchool's ongoing investigation into the root cause.

[31] For information about the earlier unauthorized activity in PowerSource. See: PowerSchool_Investigation_Report_Final.

[32] See page 162 to 170 of NIST SP 800-53, Rev.5: Security and Privacy Controls for Information Systems and Organizations.

[33] MFA can add an additional layer of security to an account or device by requiring additional verification such as a PIN or fingerprint to gain access to the account or device. Two-factor authentication is a type of

SIS and PowerSource that were in place at the time of the cyberattack, PowerSchool initially responded as follows.

[57] PowerSchool advised it has "robust authentication and password requirements". PowerSchool submitted it follows the latest NIST guidelines on password length, complexity and rotation requirements. According to PowerSchool, all employees must review its password governance policy annually. PowerSchool expects that all of its employees comply with PowerSchool's various security measures, including strong passwords in compliance with their encryption policies, thereby maintaining password complexity and length, and securing passwords through appropriate methods.

[58] Regarding MFA, PowerSchool stated that "security systems, including two-factor and MFA security systems varied across PowerSchool products and platforms".

[59] The NIST Guidance of 2025[34] indicates password length is a primary factor in characterizing password strength and sets out recommended 8 characters minimum password lengths for MFA and 15 characters minimum for single-factor authentication. I strongly recommend the institutions review PowerSchool's Password Policy to determine whether changes need to be made to strengthen the policy and technical implementation in PowerSchool's systems to meet the latest NIST standards as is reasonable in the circumstances.

[60] With respect to MFA, PowerSchool subsequently advised that, at the time of the cyberattack, "MFA did not apply to PowerSchool users logging into PowerSource". Based on the available facts, MFA was in place on the SIS, but not on PowerSource. PowerSchool explained that the lack of MFA on PowerSource was due to the portal being supported for a long period of time with multiple dependencies and PowerSource was not originally designed to support MFA.

[61] Notably, PowerSchool's Access Control Policy states "all PowerSchool accounts must have multi-factored authentication (MFA) enabled for any system which supports MFA. Where possible, all PowerSchool business systems and infrastructure should use PowerSchool SSO [single-sign-on][35] for authentication. When not possible, an exception must be requested and approved in writing by Corporate IT [information technology] and Information Security leadership".

[62] It is unclear whether PowerSchool had informed the institutions that MFA was not in place on PowerSource from the outset, but the institutions may have become aware

---

MFA. See: Secure your accounts and devices with multi-factor authentication (ITSAP.30.030) – Canadian Centre for Cyber Security.

[34] NIST Special Publication 800-63B.

[35] SSO is an authentication control system that allows users to access multiple systems using one set of credentials. SSO systems limit the storage and exposure of sensitive information such as passwords or personal information. See: https://www.cisa.gov/sites/default/files/2024-06/Barriers-to-SSO-Adoption-for-SMB-508c.pdf.

of this as users logged into PowerSource. In my view, the lack of MFA on the former subcontractor's account was a security flaw in PowerSchool's security posture and a contributing factor to the root cause of the cyberattack. As it is a best practice[36] to implement MFA for privileged accounts, such as the one used by the former subcontractor, I recommend the institutions demand PowerSchool provide evidence that, since the cyberattack, MFA has been implemented on PowerSource or any system that has similar remote connection functionality.

ii. Cloud-Based Servers and On-Premise Servers

[63] PowerSchool's SIS uses two types of servers; cloud-based or on-premises. PowerSchool stated that the institutions could choose the type of server they preferred for storage of their data. If an institution selected the cloud-based[37] option, its data would be stored on a cloud-based server. Whereas, for on-premise server, PowerSchool provides the SIS to an institution, that then stores the data on-site (locally).

[64] At the time of the cyberattack, 19 institutions used PowerSchool's cloud-based SIS server, while two institutions used an on-premise SIS server. The cloud-based servers and on-premise servers had the same access privileges in place, where a remote administrator (PowerSchool employee) or privileged user could gain entry to the institutions' data on either type of SIS server.

[65] According to PowerSchool, the institutions could give consent to allow PowerSchool to provide remote maintenance support. If consent was given, it permitted PowerSchool's technical maintenance workers to remotely access the institution's SIS. PowerSchool advised that the default selection for remote maintenance support on either cloud-based or on-premise servers is "off", although the institutions had the option to turn the feature on for a select date range or to select "always on". Further, PowerSchool submitted that the institutions could revoke access for remote maintenance support at any point. In this case, many of the institutions selected the "always on" feature and did not revoke access for remote maintenance support to their respective SIS server. Of note, PowerSchool indicated that those institutions that did not have the "always on" feature on their SIS server were not affected by this cyberattack.

[66] In this cyberattack, the threat actor accessed both cloud-based and on-premise SIS servers in cases where the remote maintenance support feature was set to either "always on" or who had allowed remote maintenance support during the time period when the threat actor had access to PowerSource. I noted that most of the institutions had agreed (consented) to PowerSchool providing such a service as set out in their Agreements, although in some cases the language was not clear.

[67] Had the institutions disabled or limited access for remote maintenance support on

---

[36] See page 132 of the NIST SP 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations.
[37] PowerSchool's Cloud-Based Hosting.

their respective SIS servers to allow access only when the institution required technical support, the magnitude of this cyberattack could have been lessened. I recommend that institutions that select this remote maintenance support option be more diligent in limiting access to their SIS on an as-needed basis only.

iii. Log Retention

[68] Regarding the institutions' log retention policies in place at the time of the cyberattack, 19 institutions confirmed having properly installed and actively maintained firewalls which included regularly reviewing and monitoring relevant logs and watching for potential cyberattacks across all their computer networks. The remaining two institutions had firewall systems in place at the time of the cyberattack, with their firewall data log retention period set between one day to seven days.

[69] PowerSchool's expert investigation report provides insight into the log retention period for PowerSchool firewalls in place at the time of the cyberattack. PowerSchool's expert noted earlier evidence of unauthorized activity in PowerSchool's environment between August 16 to September 17, 2024, using the same compromised credentials as was used in this cyberattack. However, the expert stated "it did not find sufficient evidence to attribute this activity to the Threat Actor responsible for the activity in December 2024. The available SIS log data did not go back far enough to show whether the August and September activity included unauthorized access to PowerSchool SIS data".[38]

[70] I reviewed PowerSchool's Monitoring Policy, which details security related requirements about log storage and protection, log monitoring, network monitoring and log configuration. The Monitoring Policy specifies the minimum retention period[39] of the SIS logs. PowerSchool advised that the August 2024 unauthorized incident was outside the retention period resulting in no audit logs being available to detect this incident.

[71] PowerSchool's position is that it had a "robust cybersecurity program" including dedicated resources for identity security (strong passwords for authentication, role-based access controls and validation systems), network security (intrusion detection and prevention systems), application security (regular vulnerability scanning), and data security (encryption of data in transit and at rest, as well as 24-7-365 security operations center for monitoring and responding to threats). Despite this, a threat actor went undetected. I find it particularly concerning that unauthorized activities went undetected for four months, from August until December 28, 2024 and for a further period of nine days in December of 2024 when a threat actor accessed and exfiltrated the data.

[72] In my view, collecting sufficient network and security logs is crucial evidence to help identify and investigate a cyberattack. The Canadian Centre for Cyber Security Guidance recommends retaining such logs for at least six months and 13 months for

[38] PowerSchool_Investigation_Report_Final.
[39] I will not publicly disclose PowerSchool's minimum retention period.

critical logs.[40] I recommend the institutions review their log retention policies, including PowerSchool's Monitoring Policy, to determine if adjustments are necessary to ensure that network and security logs are being retained for the appropriate amount of time.

C. Contractual Agreements between the Institutions and PowerSchool

[73] Before using a service provider to deliver information management services involving personal information under an institution's custody or control, institutions must ensure that there are reasonable measures to comply with its privacy and access obligations under the *Acts*. Section 3(3) of Regulation 823 of *MFIPPA* and section 4(3) of Regulation 460 of *FIPPA* require that such security measures be "defined, documented and put in place".

[74] Some institutions explained that, before entering into any agreement with PowerSchool, prolonged negotiations were undertaken during which the institutions carefully considered their obligations under the *Acts* and the *Education Act*. During negotiations, some institutions advised PowerSchool that they did not accept a standard agreement and instead entered into customized agreements.

[75] Some institutions themselves negotiated specific terms and conditions with PowerSchool to ensure the protection of personal information. Others indicated they hired third-party experts to review their Agreements or to conduct a risk assessment of privacy and security concerns related to PowerSchool's provision of services.

[76] Upon my request, each institution provided me with a copy of their Agreement with PowerSchool, along with supplementary documents[41] including:

- Main Services Agreement (MSA) along with supplementary documents with effective dates ranging from 2011 to 2025;
- Global Data Privacy Agreement (DPA)[42] with effective dates ranging from 2020 to 2024
- Exhibit D, Data Privacy and Security with effective dates ranging from 2020 to 2022;

---

[40] Using security information and event management tools to manage cyber security risks (ITSM.80.024) – Canadian Centre for Cyber Security.

[41] The supplementary documents provided by each institution differ and this list is not exhaustive of all the documents submitted by each institution to the IPC.

[42] In this investigation, I rely mostly on the 2024 version of PowerSchool's DPA where it states, "in case of a conflict between the MSA and this DPA regarding data processing and privacy responsibilities, this DPA prevails". I note PowerSchool's DPA is publicly available with amendments made after the cyberattack. See: PowerSchool's - 2024 Global DPA 1.1. I acknowledge that the 2024 DPA does not apply to each institution as they have their own respective Agreements, rather I refer to it as it is the most current DPA with PowerSchool.

- Certificate of Insurance, Certificate of Liability Insurance and signed Quotes;
- PowerSchool SIS Hosting Frequently Asked Questions dated August 13, 2018;
- International Organization for Standardization's Information Security Management Standard (ISO/IEC 27001:2022 or hereafter ISO Standard);
- American Institute of Certified Public Accountants (AICPA) 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus – 2022); and
- PowerSchool's Privacy Breach Response Plans or Protocols and Policies.[43]

[77] During my investigation, I reviewed each Agreement between the institutions and PowerSchool as well as the above-listed documents.

[78] As part of my assessment, I also considered previous IPC Investigation Reports[44] and the IPC's Guidance on *Privacy and Access in Public Sector Contracting with Third Party Service Providers*[45] which sets out best practices for exercising due diligence and ensuring accountability for privacy and access when planning and entering into agreements with service providers.

[79] I will not be disclosing specific details about individual Agreements. Rather I will determine whether the institutions as a whole have reasonable privacy, security, retention and destruction provisions in place to protect personal information.

[80] Of concern is that some Agreements appear outdated, dating back as far as 2011. Certain institutions do not have a signed Agreement but continue receiving services from PowerSchool by institutions reviewing and signing a quote annually, or based on a pre-determined renewal cycle, that references PowerSchool's generic MSA and/or DPA.

[81] The IPC expects that the following provisions be included in agreements between an institution and the service provider it retains to process personal information on its behalf: i) ownership of data; ii) collection, use and disclosure; iii) confidential information; iv) notice of compelled disclosure; v) subcontracting; vi) security; vii) retention and destruction; viii) audits; and ix) governing law.

i. Ownership of data

[82] An agreement should state all personal information belongs exclusively to the

[43] I note that some institutions did not provide the IPC with a copy of their privacy breach response protocol.
[44] IPC's Privacy Complaint Reports MC18-48; MC17-52; and PR16-40 and Special Investigation Report PC12-39.
[45] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.

institution.[46]

[83] All of the Agreements I reviewed provide that the institutions maintain exclusive ownership of the personal information that is managed by PowerSchool. I am satisfied that the institutions maintain the control of personal information, and it is the institutions, not PowerSchool, that own this data.

ii. Collection, Use and Disclosure

[84] An agreement should indicate that the service provider cannot collect, use, or disclose any personal information for any unauthorized purposes, unless permitted by the institution. Further, any access to or use of the institution's property, technology or information that is not necessary for the performance of PowerSchool's obligations under the agreement with the institution should be prohibited, unless expressly authorized by the institution in writing.[47]

[85] I note all of the Agreements state specifically that the data shall only be collected, used, or disclosed by PowerSchool for the purpose of fulfilling its contractual obligations to the institution, and not for any other purpose, subject to applicable laws. The Agreements also state that PowerSchool may not sell, transfer, distribute, alter or disclose information for its own benefit or purpose. This includes expressly prohibiting the use of customer data (which may include personal information) by PowerSchool for its own commercial benefit, such as advertising or marketing purposes. I am satisfied that under the Agreements, the institutions maintain control of the collection, use and disclosure of the personal information. PowerSchool cannot collect, use, or disclose the personal information for unauthorized purposes unless permitted by the relevant institution.

iii. Confidential Information

[86] An agreement should define confidential information as incorporating all personal information the institution is obligated to protect under provincial, federal or other applicable laws. The service provider should be required to keep such information confidential and secure and limit access to those who require access for the purpose of performing their duties and who are specifically permitted to receive such information under the agreement.[48]

[87] I note that most of the Agreements define confidential information as including non-public information. In some Agreements the definition of confidential information explicitly includes personal information or customer data[49] that employees and agents of

---

[46] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.
[47] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.
[48] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.
[49] I note the definition of "customer data" in some Agreements means "all data (including Personal Data), files, documents and records uploaded to a Subscription Service or transmitted to PowerSchool under this Agreement by or on behalf of Customer".

PowerSchool must keep confidential to protect the privacy of the individuals to whom the personal information belongs.

[88] While most of the Agreements do not explicitly define personal information, I am satisfied that the Agreements provide protections for confidential information, and that the personal information belonging to the institutions is included within these protections, as part of the customer data. As institutions negotiate new or revised Agreements with PowerSchool, I recommend the institutions explicitly address personal information as defined under the *Acts*.

iv. Notice of Compelled Disclosure

[89] If a situation arises where the service provider is legally compelled to disclose the institution's personal information, the agreement should indicate that the service provider must provide the institution with prompt notice to allow the institution an opportunity to seek a protective order or other appropriate remedy to prevent or limit such disclosure. Further, the service provider should limit disclosure of the institution's personal information to only those portions which the service provider is legally compelled to disclose.[50]

[90] I note that most Agreements contain the recommended provisions requiring PowerSchool to give prior notice to the institution of any legally compelled disclosure.

[91] I am satisfied that most Agreements provide protections for personal information, while also allowing for disclosure of personal information when this disclosure is required by law. For those Agreements that do not have the recommended provision of notice of compelled disclosure, I recommend that the institutions incorporate the above-noted provision within their Agreements, as they negotiate new or revised Agreements with PowerSchool. If the entire Agreement cannot be negotiated or revised at this time, I recommend that the institution and PowerSchool enter into an addendum to the Agreement to incorporate this provision.

v. Subcontracting

[92] The agreement should further specify that a service provider is not permitted to subcontract any part of the contract without prior written agreement from the institution. If certain subcontracting services are agreed upon by the institution, the subcontracting agreement should identify the subcontractor and contain the same or equivalent privacy and security obligations imposed on the subcontractor as those that apply to the service provider under the agreement.[51]

[93] I note that most of the Agreements require PowerSchool employees, agents and its subcontractors to maintain the privacy of personal information if any subcontracting

[50] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.
[51] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.

occurs and to execute a written agreement with the subcontractor confirming the above subcontracting provisions.

[94] The term "subprocessor" is defined in most of the Agreements as including "PowerSchool's subcontractors or agents, appointed by or on behalf of PowerSchool in PowerSchool's role as Processor to process Customer Data on behalf of Customer in accordance with the MSA"[52]. I am satisfied that appropriate provisions are contained in most of the Agreements to address subcontracting. I recommend that those institutions that do not have subcontracting provisions in their Agreements, incorporate the above-noted provisions within their Agreements, as they negotiate new or revised Agreements with PowerSchool. If the entire Agreement cannot be negotiated or revised at this time, I recommend that the institution and PowerSchool enter into an addendum to the Agreement to incorporate this provision.

vi. Security

[95] An agreement should require the service provider to ensure the security and integrity of all personal information in its custody. The service provider should keep the institution's personal information in a secure and separate location, safe from loss, alteration, destruction or intermingling with other records and databases. Further, it should implement, and maintain reasonable physical, administrative and technological measures and procedures to safeguard the information.[53]

[96] I note all of the Agreements require PowerSchool to implement reasonable technical and organizational measures ensuring a level of security appropriate to the risk. Many institutions provided the IPC with a supplementary document, particularly PowerSchool's DPA[54] detailing physical, administrative and technological safeguards used by PowerSchool. Some of the key provisions of the DPA are set out below:

> **Data Security.** PowerSchool agrees to abide by and maintain adequate data security measures, consistent with industry standards for digital storage of Customer Data, to protect Customer Data from unauthorized disclosure or acquisition by an unauthorized person. The general security obligations of PowerSchool are set forth below. These security measures will include, but are not limited to:
>
> **A.1.1 Passwords and Employee Access.** PowerSchool will secure usernames, passwords, and any other means of gaining access to the Services or to Customer Data, at a level meeting or exceeding the applicable standards. PowerSchool will only provide access to Customer Data to employees or contractors who require access pursuant to the MSA and this

[52] PowerSchool's DPA, 2024 version.
[53] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.
[54] PowerSchool's DPA, 2024 version.

DPA, and only on terms consistent with or exceeding the data security measures required by this DPA between the Parties.

A.1.2 Security Protocols. The Parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. PowerSchool will maintain all data obtained or generated pursuant to the MSA in a secure digital environment.

A.1.3 Employee Training. PowerSchool will provide periodic security training to those employees who operate or have access to the system. Further, PowerSchool will provide Customer with contact information of an employee whom Customer may contact if there are any security concerns or questions.

A.1.4 Security Technology. PowerSchool will employ industry standard measures to protect data from unauthorized access. The service security measures will include server authentication and data encryption. PowerSchool will host data pursuant to the MSA in an environment using industry standard security controls [that] are updated according to industry standards.

A.1.5 Monitoring. PowerSchool will log and analyze events across critical systems to identify potential threats to confidentiality, integrity, and availability of Customer Data.

[…]

A.1.9 Established Security Policies. PowerSchool will follow its established access security policies to support the confidentiality, integrity, and availability of the Customer Data against risks including but not limited to unauthorized access, collection, use, disclosure or disposal, loss, or modification. Such security arrangements will include, without limitation, reasonable physical, administrative, and technical safeguards.

[…]

[97] Regarding security training and MFA, I noted that in many of the Agreements,[55] PowerSchool requires the institutions' user(s) to complete annual cyber security training (when reasonably applicable) and to use MFA to access computer systems with PowerSchool's products as follows:

3.4 Security Training. Customer agrees to require annual cyber security training for User(s) when reasonably applicable. Customer will also require

[55] PowerSchool's MSA, 2024 version.

> User(s) to utilize multi-factor authentication to access computer systems with the Services when available within the applicable Service. Customer agrees to keep a record of such training and PowerSchool may request to see them as part of compliance verification.

[98] Conversely, it does not appear that the institutions require PowerSchool employees, agents, contractors or subcontractors (PowerSchool employees) to complete annual cyber security training and to use MFA to access their SIS and PowerSource. Rather, PowerSchool only agrees to "provide periodic security training to those employees who operate or have access to the system".[56] I recommend the institutions review and determine whether their Agreements should include specific provisions to require PowerSchool employees to complete annual cyber security training along with effective monitoring mechanisms to ensure successful completion of this training and to use MFA to access the institutions' SIS and PowerSource.

[99] Further, in some institutions' supplementary document (an addition to the Agreement), I noted a provision where if a data breach occurs, PowerSchool must notify the institution within a certain timeframe:

> **Data Breach.** In the event PowerSchool becomes aware of and objectively confirms the presence of any unauthorized or improper access to, use of and disclosure of any Customer Documents and Data, including any known or suspected security breach, data loss or other adverse event known or reasonably believed to have compromised the security, integrity, availability or confidentiality of any Customer Documents and Data in its possession or under its care and control (each a "Breach"), **PowerSchool will provide notification to Customer** within a reasonable amount of time of confirmation of the incident, **not exceeding twenty four (24) hours.** [my emphasis] PowerSchool agrees to comply with all reasonable requests from Customer in relation to such Breach and, in consultation with Customer and subject to any directions from Customer, take all reasonable steps to mitigate any harmful effect resulting from any such unauthorized access to, use or disclosure of Customer Documents and Data.

[100] As noted earlier, PowerSchool discovered the cyberattack on December 28, 2024. It appears that the cyberattack was confirmed by December 29, 2025, but notice to the institutions was provided, 10 days later, on or around January 7, 2025. Based on evidence before me, PowerSchool did not notify the institutions of the data breach within the timeframe required by certain Agreements. I note some Agreements require that notice should be given not exceeding 24 hours, 48 hours, or 72 hours upon confirmation of the

[56] PowerSchool's DPA, 2024 version.

data breach, whereas in other Agreements, no timeframe was included.[57]

[101] Considering the magnitude of this cyberattack, I acknowledge it took time for PowerSchool to investigate and take the appropriate steps to contain the cyberattack. Nonetheless, I recommend the institutions review their Agreements to ensure they contain a more consistent requirement for PowerSchool to notify the institutions as soon as feasible when a privacy breach occurs, including a cyberattack.

[102] I am satisfied that most of the institutions' Agreements with PowerSchool have organizational safeguards, including physical, technical and administrative controls in place. For those Agreements that do not have the recommended security-related provisions above, I recommend that the institutions should incorporate the above-noted provisions within their Agreements, as they negotiate new or revised Agreements with PowerSchool. If the entire Agreement cannot be negotiated or revised at this time, I recommend that the institution and PowerSchool enter into an addendum to the Agreement to incorporate this provision.

vii. Retention and Destruction

[103] An agreement should require the service provider to return all the institution's confidential information, including personal information, to the institution at or before the end of the term of the contract, with no copy or portion kept by the service provider. It should also establish an ongoing retention and destruction schedule that the service provider must follow during the life of the contract.[58]

[104] I note many Agreements had provisions relating to the return, partial disposal, and complete disposal of data upon the institutions' request or the termination of their Agreements, subject to certain other conditions set out in the Agreements.

[105] Most of the institutions generally recognized their responsibility to maintain appropriate record retention policies and procedures as required by the *Acts*, their regulations and the *Education Act*. However, few of the institutions had retention schedules set out in their Agreements.

[106] As part of my investigation, I created Figure 1,[59] below, to summarize the age of the data that was subject to the cyberattack for each institution.

---

[57] PowerSchool submitted the discovery of the cyberattack occurred on December 28, 2024, the threat actor was removed from PowerSchool's environment on December 29, 2024, and notice was given to the institutions on January 7, 2025.

[58] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.

[59] I combined current and former students and their parents or guardians in one column as the IPC was informed by an institution that their information resided in the "student table" within the SIS.

Figure 1: Age of the data at issue for each institution.[60]

Institution	Age of data at issue	
	Current and former students, and their parents or guardians	Current and former educators
Toronto District School Board	since September 3, 1985	since January 1, 2006
Peel District School Board	since 1965	since 2023
Thunder Bay Catholic District School Board	since September 2015	since September 2020
Lakehead District School Board	since 2015	since 2020
York Region District School Board	since 2005	since 2022
Brant Haldimand Norfolk Catholic District School Board	since September 1, 2009	since 2012
Near North District School Board	since September 8, 2015	since September 1, 2021
The Northwest Catholic District School Board	since 2015	since March 24, 2022
Northeastern Catholic District School Board	since 2020	since 2020
Rainy River District School Board	since 2015	since February 2020
Keewatin-Patricia District School Board	since 2015	since 2015
Superior North Catholic District School Board	since 2015	since 2019
Durham District School Board	since 1997	since 2013
Dufferin-Peel Catholic District School Board	since September 2, 2003	since September 1, 2022
London District Catholic School Board	K-12 students: since 2008 adult education students: since 1993	since 2013
Wellington Catholic District School Board	since September 1996	since 2013
Halton Catholic District School Board	since September 2015	since September 2020
Simcoe Muskoka Catholic District School Board	elementary schools: since 2003 secondary schools: since 1984	elementary schools: since 2003 secondary schools: since 1984
Ottawa Catholic School Board	since 1998	since 1998
Superior-Greenstone District School Board	since September 1, 2015	since September 1, 2015
Ministry of Education	since 1999	since 1999

[60] This table accounts for the earliest year of impact reported by each institution to the IPC.

[107] I note the age of some of the data at issue dates back as far as September 1965. Many institutions readily acknowledged that certain data used during a student's or educators' tenure with the institution is no longer useful once they have left the institution. Had this outdated data been securely destroyed, following reasonable retention schedules, it would not have been included in the data that was subject to the cyberattack.

[108] Given certain data stored on PowerSchool's SIS environments goes back as far as 60 years, I strongly recommend that all institutions review and develop their data retention schedules, if not already done, and securely destroy any data holdings that exceed reasonable retention periods in accordance with the *Acts* and their regulations. I also recommend the institutions incorporate a reasonable retention schedule within the Agreements, as they negotiate new or revised Agreements with PowerSchool, to provide a framework for PowerSchool to follow and that can be enforced by the institutions. If the entire Agreement cannot be negotiated or revised at this time, I recommend that the institution and PowerSchool enter into an addendum to the Agreement to incorporate the retention schedule, the requirement for PowerSchool to follow the retention schedule, and other related provisions.

viii. Audits

[109] An agreement should require the service provider to undergo annual audits for privacy and security compliance and specify who will be conducting such audits, as well as when and how the audits will occur. In addition, the agreement should require the service provider to conduct reviews of privacy impact assessments (PIAs), threat risk assessments and other vulnerability assessments at specified times during the term of the agreement.[61]

[110] I note most Agreements contained provisions requiring PowerSchool to complete annual risk assessments, audits and compliance reports, as follows:

> **A.1.8 Periodic Risk Assessment.** PowerSchool acknowledges and agrees to conduct digital and physical periodic risk assessments at least annually and take commercially reasonable industry standard steps to remediate identified security and privacy vulnerabilities in a timely manner. PowerSchool shall provide reasonable assistance related to the nature of Processing to Customer in the event that a data protection impact assessment be required by Applicable Law.
>
> […]
>
> **A.1.10 Audits and Compliance Reports.** PowerSchool's security compliance is assessed by independent third-party auditors. Upon Customer agreeing to an NOA [Notice of Agreement], PowerSchool shall provide

[61] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.

> access to information regarding PowerSchool's ISO 27001:2022 certification and SOC II Reports. To the extent that PowerSchool discontinues a third-party audit, PowerSchool will adopt or maintain an equivalent industry-recognized security standard.

[111] I am satisfied that most Agreements contain privacy and security protections requiring PowerSchool to undergo annual audits and security compliance assessments by third-party auditors. For those Agreements that do not have the recommended provision of audits, I recommend that the institutions should incorporate audit related provisions within their Agreements, as they negotiate new or revised Agreements with PowerSchool. If the entire Agreement cannot be negotiated or revised at this time, I recommend that the institution and PowerSchool enter into an addendum to the Agreement to incorporate these provisions.

[112] Further, the IPC recommends institutions maintain an up-to-date understanding of the cyber threat landscape and require that their service provider's privacy and security protections have reasonable safeguards in place. The institutions should consider relevant industry standards and best practices for cybersecurity (such as the NIST Cybersecurity Framework, the ISO standard (ISO/IEC 27001), and the Center for Internet Security Critical Security Controls).[62]

ix. Governing Law

[113] Agreements with service providers should identify the relevant privacy laws that apply to the service provider's services, including whether more than one law is applicable and how the requirements of Ontario's privacy laws will be met.[63]

[114] Threats to privacy and security can arise at any time, and the same threat can cross multiple jurisdictions.[64] This cyberattack affected institutions in Ontario, as well as other provinces and territories across Canada, and throughout the U.S. Further, PowerSchool is a US-based corporation with data stored in cloud-based technology servers and data centers across various jurisdictions.

[115] I note many Agreements specify either *FIPPA* or *MFIPPA* as one of the governing laws, while others have general provisions in place indicating that the applicable laws depend upon the institution's location.

---

[62] Providing evidence of an information security management system meeting ISO 27001 standards, or the American Institute of Chartered Public Accountants SOC 2 Type II reports are intended to provide detailed information and assurance about the controls at an organization. Specifically related to security, availability, and processing integrity of the systems the organization uses to process users' data and the confidentiality and privacy of the information processed by these systems. These reports can play an important role in oversight of the organization, vendor management programs and regulatory oversight. See: How to Protect Against Ransomware | IPC.

[63] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.

[64] See page 7 of A Special Investigation Report PC12-39.

[116] I observed that many of the Agreements refer to compliance with *PIPEDA* which governs service providers such as PowerSchool. I also note that the Agreements identify certain international privacy laws as also being applicable.

[117] I am satisfied that many Agreements contain reference to either one or both of the *Acts*. Given this, I find the governing law identified in the Agreements includes the laws of Ontario. For those Agreements that do not have the recommended governing law provision for interpreting and enforcing the agreement, I recommend that the institutions incorporate the above-noted provision within their Agreements as they negotiate new or revised Agreements with PowerSchool. If the entire Agreement cannot be negotiated or revised at this time, I recommend that the institution and PowerSchool enter into an addendum to the Agreement to incorporate this provision.

Overall conclusions on the content of the Agreements between the Institutions and PowerSchool

[118] To ensure the privacy and security of the personal information at issue, the Agreements should contain provisions requiring PowerSchool to have in place reasonable and appropriate measures ensuring the institutions' compliance with the *Acts* and their regulations.

[119] Overall, I find most of the Agreements require PowerSchool to have reasonable measures in place to ensure the privacy and security of personal information. I do, however, have concerns with those Agreements that are outdated or lack the recommended provisions addressing subjects such as confidential information, notice of compelled disclosure, subcontracting, security, retention and destruction, audits, and governing laws. I recommend the institutions review their Agreements with PowerSchool to ensure they include the above-noted provisions rather than merely accepting PowerSchool's standardized agreements and supplementary documents.

D. Monitoring and oversight measures to ensure compliance with the terms of the Agreements

[120] When using a service provider, institutions must not only have adequate contractual agreements in place with their service providers, but they must also take reasonable oversight measures to ensure the service provider complies with the terms of such agreements.

[121] Notably, institutions should take reasonable actions, including regular follow-ups to monitor the service provider's performance against the defined terms and conditions set out in the agreement for the duration of the agreement. Institutions should require proper documentation from their service provider and take appropriate measures to enforce the contract. For example, this includes demanding the service provider to comply with its privacy and security obligations and take necessary remedial measures to correct any deficiencies promptly or risk termination of the contract.

[122] As part of my investigation, I asked each institution to describe how they ensure PowerSchool is complying with its contractual obligations in relation to privacy and security measures. Most institutions advised they do not have a formal system in place to regularly monitor or oversee PowerSchool's compliance with the provisions set out in their Agreements. Many institutions acknowledged that their Agreements, and supplementary documents, are only reviewed when a service issue arises with PowerSchool.

[123] As part of the institutions' accountability responsibilities, they should define and document their oversight and monitoring measures including obtaining evidence of compliance to hold PowerSchool accountable for commitments set out in the Agreements.

[124] At minimum, institutions should be able to request and receive copies of relevant PowerSchool policies, completed certifications and audit reports as well as other relevant documents attesting to PowerSchool's compliance with the terms and conditions of the Agreements.

[125] At the outset, many institutions referenced broad statements from PowerSchool's website[65] indicating PowerSchool was certified in 2022 as meeting industry cybersecurity standards, specifically, SOC 2 and the ISO standard.[66] Most institutions submitted to the IPC that, based on these statements, they concluded PowerSchool "must have demonstrated to third-party auditors it had reasonable technical measures in place to preserve [an institution's] data integrity and data confidentiality".

[126] Without sufficient evidence, I was unable to determine the adequacy of PowerSchool's compliance with the SOC 2 framework and the ISO standard. To verify such compliance for SIS and PowerSource, I requested the institutions to provide details of the most recent audit reports conducted by a third-party independent auditor before the cyberattack, specifically a SOC 2 audit report and ISO standard surveillance and recertification audit report (collectively, the Audit Reports).

[127] According to the institutions, the Audit Reports are posted on a "regular basis" to a named account[67] that can be accessed by the institutions. One institution advised that PowerSchool periodically posts updates to the Audit Reports on the account, but PowerSchool does not issue notifications to the institutions informing them that the Audit Reports have been posted. This means that institutions must regularly login to the named account to proactively monitor and review the Audit Reports to know whether any deficiencies were identified by the auditors and what steps PowerSchool needs to take to

---

[65] I note PowerSchool updated its website after the cyberattack providing additional details about its security posture to the public.

[66] To renew ISO 27001 certification, organizations are required every three years to have a recertification audit completed. In this case, PowerSchool was certified in 2022 and as of November 12, 2025, PowerSchool reported to the IPC that it has undergone recertification in 2025 to maintain its ISO 27001 certificate.

[67] I will not specify the name of the account due to security risks.

address these.

[128] According to PowerSchool, an auditor conducts annual examinations on PowerSchool's core products to confirm ongoing compliance with the SOC 2 framework and ISO standard and then provides audit reports to PowerSchool. PowerSchool advised that the 2024 audit reports concluded that PowerSchool's controls were "strategically modified and implemented to mitigate any vulnerabilities, deviations and control gaps identified through various evaluations, such as risk assessments and vulnerability scans". At the time of this investigation, it appears that the 2024 Audit Reports had not been posted to the named account and were therefore not available to the institutions.

[129] At my behest, the institutions requested the 2024 Audit Reports from PowerSchool, however, PowerSchool advised that the audit reports are confidential and would not be disclosed without assurances of confidentiality from the institutions and the IPC.

[130] It is concerning that despite most Agreements stating, "Upon Customer agreeing to an NOA [Notice of Agreement], PowerSchool shall provide access to information regarding PowerSchool's ISO 27001:2022 certification and SOC II Reports",[68] PowerSchool would not provide the institutions with the 2024 audit reports until the IPC intervened. Based on the available evidence before me, PowerSchool claims that the Audit Reports are periodically posted on a named account which the institutions have access to, but in this case, only one of the Audit Reports (SOC 2 Type 2 Audit Report) was apparently posted to the named account.[69] Be that as it may, the institutions were still unable to obtain these audit reports upon my request to confirm that annual audit reports were being completed by PowerSchool in compliance with the SOC 2 and ISO standards. The institutions were not able, therefore, to exercise the necessary oversight to ensure PowerSchool was meeting its obligations under the Agreements, nor were they able to enforce the provision requiring PowerSchool to provide them with copies of relevant Audit Reports and certifications upon request to prove compliance.

[131] PowerSchool ultimately provided me with the requested information on assurance that the IPC would not publish confidential and sensitive information where the disclosure of that information may pose a security risk to an organization. The ISO Standard Surveillance Audit Report[70] of July 16, 2024 provided by PowerSchool indicates that the audit was designed to determine continuing conformity with the requirements of the ISO standard. Based on the evidence before me, it appears PowerSource and SIS were within scope of the ISO Standard Surveillance Audit Report confirming ISO standard compliance

[68] Section A.1.10 of PowerSchool's DPA, 2024 version.
[69] PowerSchool advised in its November 12, 2025 representations that the SOC 2 Type 2 Audit Report relating to SIS was posted to the named account in or about October 2024. Based on the available evidence, it is unclear whether this report was posted.
[70] The ISO standard surveillance audit report is conducted annually by a third-party auditor to ensure an organization remains compliant and maintains effective security controls according to the ISO standards. The auditor will check for any nonconformities during the audit for the organization to address.

with no non-conformities for the period between June 10 to June 21, 2024.

[132] I also reviewed the SOC 2 Type 2 Audit Report provided by PowerSchool and note that it was completed by an auditor in accordance with standards established by the AICPA[71] (a non-profit professional association that sets standards for auditing), covering the period of July 1, 2023 to June 30, 2024. The auditor provided PowerSchool an opinion on the description, suitability of design and operating effectiveness of controls based on the auditor's examination of certain PowerSchool named technologies, including Powerschool's SIS. Notably absent from these technologies however is PowerSource, which is not identified as having been examined within the scope of the SOC 2 Type 2 audit report.

[133] Further, I asked PowerSchool to provide details of the penetration and vulnerability testing on SIS and PowerSource, including the reports created before the cyberattack. In my review of the Penetration Testing Summary Report dated June 25, 2024, I note it was conducted by a third-party service provider engaged by PowerSchool to identify security vulnerabilities in certain named PowerSchool technologies. The report rates each security vulnerability for technical impact, along with recommendations for PowerSchool to implement.

[134] I note the scope of the Penetration Testing Summary Report includes SIS for the period of April 30 to June 25, 2024, but once again, PowerSource is not included.

[135] According to PowerSchool's Vulnerability Management Policy, "(a)ny PowerSchool application with active customers must have [an] annual penetration test performed". In my view, PowerSource has "active customers" (including active users from the institutions accessing or receiving technical support through this customer support portal at the time of the cyberattack),[72] yet I was not provided with any evidence that PowerSchool conducted or conducts annual penetration testing on PowerSource.

Overall conclusions regarding monitoring and oversight measures

[136] Given the above, it is my view that the institutions generally did not demonstrate adequate efforts to diligently monitor PowerSchool's compliance with the reasonable security measures required by the Agreements, specifically regarding access privileges for user accounts and systems, MFA for SIS and PowerSource, log retention periods, compliance with retention schedules, audit reports and vulnerability assessments covering both SIS and PowerSource. Further, it does not appear the institutions monitored the breach notification provisions in their Agreements to ensure PowerSchool complied within a consistent timeframe to provide notice in accordance with the breach

[71] About us | Resources | AICPA & CIMA.

[72] PowerSource's website uses terms such as "pre-sales customers" and "existing customers" and "available to all district and school staff, including teachers, administrators and IT staff", which in my opinion shows this customer support portal for all PowerSchool products had "active customers" at the time of the cyberattack. See: PowerSource; and PowerSource - Need a PowerSource account?

notification provisions.

[137] The institutions are responsible for monitoring PowerSchool's compliance with the privacy and security commitments and obligations set out in their Agreements. If the institutions become aware of gaps or inefficiencies in PowerSchool's data management services, the institutions must be able to follow-up to ensure that PowerSchool takes reasonable and timely action to address them.

[138] In my view, the institutions lack sufficiently robust enforcement provisions in their Agreements with PowerSchool to require compliance (or if they did, failed to exercise them), as was evidenced by their inability to obtain the latest audit reports from PowerSchool despite a clear contractual provision giving them this right.

[139] From the available facts, I find the institutions did not have reasonable security measures in place to prevent unauthorized access to the personal information in their custody or control, as required under the *Acts* and their regulations. When negotiating new or revised Agreements with PowerSchool, I recommend the institutions add sufficiently robust enforcement provisions that create penalties or other clear consequences for PowerSchool's non-compliance with contractual terms and that the institutions act decisively in exercising these provisions, including in respect of Powerschool's obligation to provide documents upon request.

Issue 2: Did the institutions, as a whole, respond adequately to the breach?

[140] The IPC's *Privacy Breaches: Guidelines for Public Sector Organizations* (Privacy Breach Guidelines)[73] sets out best practices for institutions to respond to privacy breaches, including a cyberattack.

[141] When a breach occurs, the Privacy Breach Guidelines recommend steps institutions should take to identify the scope and contain the breach, assess whether the breach creates a real risk of significant harm (RROSH), notify those impacted, report the breach to the IPC and other relevant entities, investigate and reduce the risk of a future breach.[74]

[142] Determining whether a breach creates a RROSH to affected individuals includes assessing the following factors:

- the sensitivity of the personal information involved
- the probability that the personal information has been, is being, or will be, misused
- the availability of steps the individual could take to reduce the risk of the harm occurring or mitigate the harm should it occur[75]

[73] Privacy Breaches: Guidelines for Public Sector Organizations | IPC.
[74] Privacy Breaches: Guidelines for Public Sector Organizations | IPC.
[75] Privacy Breaches: Guidelines for Public Sector Organizations | IPC.

i. Privacy Breach Response Plan or Protocol

[143] Upon discovery of a breach, including a cyberattack, institutions should take immediate steps to respond to the breach. All public sector institutions should have a documented privacy breach response plan (or protocol)in place to help them respond immediately.

[144] A robust breach response plan should clearly set out the roles and responsibilities of specific staff positions within the organization that comprise the breach response team. This team should include experts from different areas on an as needed basis. Institutions should practice responding to breaches periodically through simulated exercises (for example, tabletop exercises) to ensure everyone understands their roles if and when a breach occurs and that they act in a timely and coordinated manner.[76]

[145] Most of the institutions provided a copy of their breach response plans to the IPC, along with supplementary documents setting out their obligations under the *Acts*, that were in effect at the time of the cyberattack. As part of my investigation, I reviewed these documents.

[146] I note that many of the institutions had robust breach response plans that also addressed breaches involving their service provider. These breach response plans had structured approaches and response processes, including the identification of the scope of the breach, the containment of the breach, the removal of a threat actor from the institution's system(s), the recovery of data, the notification of affected individuals, regulators and involved parties (such as law enforcement), and the documentation of lessons learned. These breach response plans also set out roles and responsibilities for individuals in specific staff positions when responding to a breach. Some of the institutions even had a cybersecurity breach checklist.

[147] Other institutions recognized improvements could be made to their breach response plan and some lacked reference to breaches involving their service providers. More concerning is that one institution acknowledged not having a breach response plan at all.

[148] To better adapt to evolving cybersecurity threats, institutions should ensure their breach response plans and cybersecurity policies and procedures are regularly reviewed, tested and updated to tackle new and evolving threats. This includes creating a defined and documented breach response plan involving the institutions' service provider that can be followed if and when a breach occurs.

[149] When an institution contracts with a service provider, as was the case here, the institution is responsible for ensuring the service provider also has a breach response plan in place. Provision(s) requiring this should be set out in the contract between an

[76] Privacy Breaches: Guidelines for Public Sector Organizations | IPC.

institution and the service provider.

[150] To confirm that PowerSchool had a breach response plan in place at the time of the cyberattack, I asked the institutions to describe PowerSchool's breach response plan in detail including any changes made to it as a result of this cyberattack, and to obtain a copy. Initially, PowerSchool did not provide a copy of its Security Incident Response Procedure to the institutions, taking the position that it is confidential as it contains critical information about its internal security posture and infrastructure.

[151] Certain institutions informed PowerSchool that its response was inadequate as it did not comply with the following provision, set out in their Agreements:

> "PowerSchool further acknowledges to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and provincial law for responding to a data breach, breach of security, privacy incident, or unauthorized acquisition or use of the Customer Documents and Data or any portion thereof, including personally identifiable information and **agrees to provide Customer, upon request, with a copy of said written incident response plan**." [my emphasis]

[152] After multiple requests to PowerSchool from the IPC and the institutions, PowerSchool ultimately provided its Security Incident Response Procedure to the IPC. PowerSchool advised that limited changes were made to the Security Incident Response Procedure after the cyberattack and provided a version reflecting these changes. I note that two institutions informed the IPC that they did not receive the revised Security Incident Response Procedure from PowerSchool.

[153] Given the above, I recommend that these institutions review their own breach response plans, and related protocols, policies and practices to determine whether changes are needed in light of this cyberattack, including in respect of third-party service providers. In the case of the one institution that does not have a breach response plan at all, I recommend that it creates and implements one as soon as possible.

[154] I also remind the institutions that, under their respective Agreements, they have the authority to ensure PowerSchool has a robust Security Incident Response Procedure in place. I recommend the institutions periodically request a copy of PowerSchool's Security Incident Response Procedure and review it to confirm consistency with relevant industry standards that are reasonable in the circumstances to ensure compliance with the institutions' breach response obligations under the *Acts* and determine whether any changes need to be made to PowerSchool's procedure accordingly.

ii. Determining the Scope

[155] As discussed above, after the discovery of the cyberattack, PowerSchool's cybersecurity experts determined the scope and extent of its impact. PowerSchool then

informed the affected institutions about the cyberattack.

[156] Upon being informed of the cyberattack by PowerSchool, institutions initiated their own breach response plans which included reporting the cyberattack to their insurer, the ministry, law enforcement and the IPC. Simultaneously, institutions engaged experts, and many retained third-party cybersecurity counsel.

[157] The institutions conducted their independent investigations verifying what data was involved in the cyberattack and reviewed their own computer networks at large to confirm there was no lateral impact to their non-PowerSchool infrastructure. The institutions also communicated with PowerSchool regarding their affected data and received assurances from PowerSchool that the SIS environment and PowerSource were safe to use going forward.

[158] As noted above, the affected information in this investigation relates to three groups of individuals: current and former students, their parents or guardians, and current and former educators.

[159] The affected information relating to current and former students includes some or all of the following:

- name, gender, home and/or mailing address, telephone number, residency status, place of birth;
- date of birth, health card number, social insurance number (SIN);
- Ontario Education Number, student number, board email address, Education Quality and Accountability Office accommodation information,
- school information (initial, recent and next school enrollments, grade level, homeroom class name, board entry and exit dates, start and end dates of the school year, reasons for transferring between schools, admission and withdraw codes, graduation school with date and year);
- First Nations, Metis, Inuit status;
- medical information (allergies, medical conditions, injuries, physicians' name and telephone number), insurance policy information;
- family information (sibling association, emergency contact information, custodian information, designated individual(s) to pickup student);
- other information (other alerts, assessments, individualized education program references, locker number and combination); and
- principal or vice principal notes (discipline notes).

[160] The affected information relating to parents or guardians includes some or all of the following:

- names, home address, telephone numbers, email addresses; and
- relationship to student.

[161] The affected information relating to current and former educators included some or all of the following:

- name, gender, personal phone number and home address; and
- SIN; job title, employee number, board email address, homeroom class, department, current job status, school(s) of employment, Ontario College of Teachers number, ministry number.

[162] Considering the sensitivity of the personal information, the probability that the personal information has been or will be misused, and the availability of steps the individual could take to reduce the risk of the harm or mitigate the harm should it occur, I find that the cyberattack of the personal information at issue in this case creates a RROSH to those affected.

[163] When I asked certain institutions why students' health card numbers, SINs and insurance policy numbers were collected and to specify the authorized purpose for the collections under applicable laws or regulations, most institutions acknowledged these collections were unauthorized, contrary to section 38(2) of *FIPPA* and 28(2) of *MFIPPA*.

[164] One institution advised that students' health card number was historically collected during student registration as an "optional field" where parents or guardians could voluntarily provide this information to be used if a medical emergency occurs at school.

[165] Five institutions acknowledged the collection of SINs was done by administrative staff members who had inputted them into their respective SIS, without authorization.

iii. Notifying Law Enforcement

[166] Only three institutions in this case directly reported this cyberattack to Ontario law enforcement agencies, while the remaining 18 institutions relied upon PowerSchool to take this step. Some institutions acknowledged being unaware as to who is responsible -- the institution or PowerSchool -- for notifying Ontario law enforcement agencies, particularly for a cyberattack of this nature.

[167] Initially, PowerSchool advised that it reported the cyberattack directly to law enforcement agencies in the US and Canada, as well as the Canadian Centre for Cyber Security. When I asked the institutions to specify which law enforcement agencies PowerSchool contacted, PowerSchool acknowledged to the institutions that its reporting

was limited to US law enforcement agencies and that it did not directly report this cyberattack to any agencies in Ontario. PowerSchool stated that it understood that the US agencies coordinated reporting with Canadian agencies.

[168] In my view, where a cyberattack involves a suspected crime that affects sensitive information of a large number of Ontarians amounting to a RROSH, institutions should coordinate with their service provider to ensure a direct report is made to appropriate Ontario law enforcement agencies. I recommend that steps be taken to notify Ontario law enforcement agencies as this may help to assist in an investigation.

iv. Breach Containment

[169] As part of the institutions' containment measures after the cyberattack, the fields containing students' health card numbers, SINs and insurance policy numbers were removed from their SIS. Some institutions submitted the above information was deleted, is no longer being collected, and no new entries for these types of personal information can be entered into their SIS. Further, institutions educated their staff about the institutions' relevant policies and procedures and the change in practice to cease collection of these types of personal information. I strongly recommend that *all* institutions must cease unauthorized collection of personal information, including personal information that is not necessary for delivering their education mandate, including health card numbers, SINs and insurance policy numbers.

[170] One institution did not provide the IPC with details of its containment measures involving its SIS. If it has not already done so, I recommend this institution take prompt and reasonable steps to contain the affected data within its SIS and notify those affected individuals of the containment measures taken.

[171] To confirm that the threat actor did not enter the institutions' networks, PowerSchool provided the malicious internet protocol (IP) addresses used by the threat actor to the institutions. These IP addresses contain digital and contain information clues (often called indicators of compromise (IOCs))[77] are used to help the institutions detect suspicious activity within their networks.

[172] In response, the institutions immediately reviewed their network and security logs to search for the presence of these IP addresses. Certain institutions used the malicious IP addresses to continuously monitor for any activity from these IP addresses in their networks. Others engaged third-party forensic investigation experts to perform a forensic analysis of the institutions' networks. These experts' findings aligned with PowerSchool's Investigation Report.[78] Some institutions had their information technology departments review the export data logs on their SIS, review the IOCs on their firewalls, and conduct user audits. According to all of the institutions, they did not find any further unauthorized

[77] IOCs are digital artifacts suggesting a cyberattack is imminent or is currently underway or that a compromise may have already occurred. See: Indicator of Compromise - Glossary | CSRC.
[78] PowerSchool_Investigation_Report_Final.

activity, nor did they find any evidence that the threat actor entered their respective internal networks.

[173] Regarding PowerSchool's containment measures, PowerSchool advised the IPC that the threat actor was removed from the PowerSchool environment on December 29, 2024. As the threat actor accessed SIS through PowerSource, PowerSchool took further containment steps by moving PowerSource to a secure enclave with additional restrictions, including a firewall. PowerSchool also deactivated the compromised credential, enforced a full password reset for employees and contractors and restricted access to and tightened password and access controls for PowerSource.

[174] Notwithstanding that there are no guarantees that there will never be any further ramifications resulting from this cyberattack, I am satisfied the institutions adequately determined the scope of the cyberattack and took reasonable steps to contain it as much as possible, in coordination with PowerSchool.

v. Notification of Affected Individuals

[175] The IPC's *Privacy Breach Guidelines* recommend that when a breach, including a breach resulting from a cyberattack, affects a service provider contracted by an institution to process personal information on its behalf, institutions should ensure their service provider informs them about the breach immediately.[79] In this case, PowerSchool did not inform the institutions about the cyberattack immediately, but rather 10 days later.

[176] Once informed by the service provider, it is the institution's responsibility to notify affected individuals as soon as feasible after a breach, where the institution determines that the breach poses a RROSH to affected individuals.[80]

[177] The IPC generally recommends that institutions notify affected individuals of a breach through direct notice by a telephone call, letter, email, or in person.[81]

[178] Indirect notice can be used where direct notice is not reasonably practical or possible. For instance, when the breach affects a large number of individuals, where there is outdated contact information, or where direct notice would result in unreasonable interference with the operations of an institution.[82]

[179] When using indirect notice, a prominent notice should be displayed on the institution's website and other media channels with details about the breach. Distribution of the notice should be done using multiple methods, including through media announcements, social media posts, public outreach activities, or other means that could

---

[79] Privacy Breaches: Guidelines for Public Sector Organizations | IPC.
[80] As of July 1, 2025, *FIPPA* requires institutions to notify affected individuals of privacy breaches that pose a RROSH as soon as feasible after determining the breach occurred. It is a best practice for institutions subject to *MFIPPA* to also follow this as guidance.
[81] Privacy Breaches: Guidelines for Public Sector Organizations | IPC.
[82] Privacy Breaches: Guidelines for Public Sector Organizations | IPC.

help raise awareness of the breach.[83]

[180] Further, notice (direct or indirect) should include, among other things, a statement advising whether the institution has reported the matter to the IPC and as required by section 40.1(4) of *FIPPA*, a statement that an affected individual has a right to make a complaint to the IPC, information on how to do so and advising that the time limit for filing the complaint is within one year.[84]

[181] Initially, many of the institutions provided the IPC with draft versions of their notification strategies, involving a combination of direct and indirect notifications. Given the above-mentioned notification recommendations and requirements and the large number of affected Ontarians, the IPC requested the institutions to include a statement in their notices that, "[t]his breach has been reported to [the IPC] and an investigation file has been opened. While you are entitled to file a complaint, the IPC has advised that it is not necessary as they are already investigating the matter. You can visit the IPC's website…." All of the institutions agreed and included similar statements in their notices.

[182] Throughout January 8 to May 7, 2025, institutions issued indirect notices regarding the cyberattack on the institutions' respective websites and through internal communication broadcasts, press releases, and posts on social media platforms and media channels.

[183] Notices included details about the extent of the cyberattack, specifics of the affected personal information, steps taken to address the cyberattack and confirmation that the IPC as well as other agencies were notified. Each institution provided an email address or contact information for people to direct their inquiries or concerns. The institutions also provided details about a call center managed by PowerSchool for this cyberattack. Certain institutions provided details and enrollment instructions to affected individuals regarding identity protection and credit monitoring services being offered by PowerSchool, while others directed the individuals to PowerSchool's website to obtain additional information.

[184] Most institutions published Frequently Asked Questions (FAQs) and regularly updated their notices and the FAQs on their websites.

[185] Some institutions issued certain notifications directly by way of a telephone call, letter and/or email to individuals whose affected personal information included health card numbers, SINs, insurance policy numbers, and where contact information for these individuals was current and available. I am satisfied with the institutions' efforts to provide direct notification to affected individuals, where reasonably possible.

[186] Given the unfortunate age of some of the affected personal information, I am

---

[83] Privacy Breaches: Guidelines for Public Sector Organizations | IPC

[84] To understand which information should be included in direct and indirect notifications to affected individuals. See: Privacy Breaches: Guidelines for Public Sector Organizations | IPC.

mindful of the fact that the institutions may not have up-to-date contact information for many of the affected individuals. As such, I am satisfied that the institutions' efforts to provide indirect notification to these individuals was reasonable. For the most part, these indirect notices were clear and readily visible and accessible on their respective websites.

[187] However, on reviewing certain institutions' websites, I note their indirect notices were somewhat buried, potentially limiting accessibility for those impacted. Given this, I recommend the institutions ensure that any future indirect notices be placed more prominently on their websites (or other media channels) to increase the effectiveness of their public outreach.

vi. Investigation into the Cause of the Breach

[188] PowerSchool submitted that it retained an industry-leading cybersecurity expert to investigate the cyberattack, the investigation began on December 29, 2024 and ended on February 17, 2025. Further, the cybersecurity expert's findings revealed that the compromised credentials were still valid at the time of the cyberattack.

[189] Early in my investigation, I reviewed PowerSchool's Investigation Report.[85] I subsequently requested a more detailed report from the institutions because I found the Investigation Report lacked critical security information related to the root cause of the cyberattack, details about the compromised credentials, and insufficient information about the lack of MFA on PowerSource. In turn, PowerSchool stated it "does not have any additional non-privileged reports" and many institutions also noted PowerSchool's refusal to produce such reports to them. In its November 12, 2025 response to a draft version of this report, PowerSchool submitted that "full forensic reports are highly confidential; public disclosure could undermine the effectiveness of PowerSchool's privacy and security controls".

[190] To the extent such forensic reports exist in regard to this incident, the institutions should be able to demand and receive from PowerSchool information and facts from these reports. This expectation would be entirely consistent with many Agreements that require PowerSchool to comply with all reasonable requests from the institutions when a data breach occurs. The relevant provision requires that PowerSchool:

> B.2.2 comply with all reasonable requests from Customer in relation to such Incident and, in consultation with Customer and subject to any directions from Customer, take all reasonable steps to mitigate any harmful effect resulting from any such unauthorized access to, use or disclosure of Customer Data.[86]

[191] Notably, many Agreements also include provisions that place specific post-incident

[85] PowerSchool_Investigation_Report_Final.
[86] PowerSchool's DPA, 2024 version.

obligations on PowerSchool, such as the following:

> B.3.3 PowerSchool agrees to adhere to all requirements in applicable state, provincial and federal law with respect to an Incident related to Customer Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation, where commercially reasonable, of any such data breach.
>
> […]
>
> B.3.5 If Customer requests PowerSchool's assistance providing notice of unauthorized access, and such assistance does not take on a form unduly burdensome to PowerSchool, PowerSchool will reasonably cooperate and assist in, any investigation of a complaint that any Customer Data has been collected, used or disclosed contrary to Privacy Laws, or the policies of Customer, whether such investigation is conducted by Customer itself or a body having the legal authority to conduct the investigation, including but not limited to co-operation and assistance in notifying the affected Data Subject(s) of the unauthorized access.[87]

[192] In my view, PowerSchool did not fully comply with the multiple requests for information from the institutions despite the above-noted provisions in the Agreements requiring PowerSchool provide such information after a data breach and as part of the post incident process. I recommend that the institutions pursue all necessary means against PowerSchool (including legal means, if and as necessary) to access forensic investigation reports and/or facts from such reports in regard to this or any breach or cyberattack, affecting personal information in the institution's custody or under its control.

[193] Considering it took over four months for PowerSchool to detect a threat actor in its environment, I also recommend that the institutions require PowerSchool to regularly review its early breach detection process to ensure more proactive strategies are in place to identify a cyberattack in its initial stages.

vii. Remediation Steps by the Institutions

[194] As a result of this cyberattack, many institutions are creating or revising their own cybersecurity-related breach response plans and supplementary documents that apply to all of their systems. Institutions with existing breach response plans have advised the IPC that their breach response plans are now being reviewed annually with lessons learned from this cyberattack to be included in their 2025 review. I recommend *all* the institutions take the necessary steps to develop robust breach response plans.

[195] Regarding amendments to their Agreements, certain institutions have advised that they will collectively request PowerSchool to revise their Agreements. No timeframe has

[87] PowerSchool's DPA, 2024 version.

been given to the IPC for the completion of these revisions. I recommend that *all* the institutions revise their Agreements with PowerSchool, as needed, to address the shortcomings identified in this report.

[196] Many institutions advised they are collaborating within the education sector to ensure adoption of similar contracting processes and practices. Certain institutions indicated that third-party risk management guidance and resources may be collaboratively prepared by representatives from the ministry, the Ministry of Public and Business Service Delivery and Procurement, and multiple Ontario school boards. Moreover, 19 institutions have advised they are formalizing an internal process to significantly align with the IPC's guidance, *Privacy and Access in Public Sector Contracting with Third Party Service Providers*[88] and will apply it to their electronic data management service providers.

[197] Most institutions advised they will be annually reviewing PowerSchool's compliance with their Agreements, including requesting and reviewing copies of any vendor audit reports. Many of these institutions advised they are taking additional proactive measures to address any gaps identified by the audit reports. I recommend *all* the institutions do the same.

[198] Regarding retention and destruction of the data, many institutions advised they are developing a data retention policy and comprehensive records retention procedures to comply with the *Acts* with anticipated implementation for the 2025-2026 school year. I recommend *all* the institutions do the same.

[199] One institution advised the IPC that it is undergoing a review of the affected personal information that should be removed from its SIS to comply with the relevant privacy laws. This undertaking will then lead to an annual purging process for this institution to remove "unnecessary data". For instance, if this institution assesses and determines that a former student's medical notes, home address, phone number is no longer needed, the data will be purged accordingly. I recommend *all* the institutions undertake the same exercise to purge unnecessary personal information.

[200] Regarding log retention, two institutions are improving their security infrastructure and the time period which security logs are retained. I recommend *all* the institutions do likewise.

[201] As of July 1, 2025, it is an explicit and mandatory requirement for institutions subject to *FIPPA,* including the ministry, to conduct a PIA.[89] As a best practice, going forward, one institution stated it will audit and conduct a PIA and cyber risk assessment on PowerSchool services on an annual basis. I recommend *all* of the institutions, including those subject to *MFIPPA*, carry out a PIA in accordance with the institutions follow the

[88] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.
[89] FIPPA, s. 38(3).

IPC's *Planning for Success: Privacy Impact Assessment Guide*[90] to ensure appropriate identification, assessment and mitigation of any potential risks to personal information.

viii. Remediation Steps by PowerSchool

[202] Following the cyberattack, PowerSchool advised it took remedial action to strengthen its cybersecurity posture by:

- implementing biometric authentication across its organization in or about July 2025;
- investing in physical security measures including fingerprint and facial recognition authentication for all employees and contractors;
- requiring all PowerSchool employees and contractors to use single-sign-on, MFA, virtual private network, and desktop virtualization to access all PowerSchool environments, including SIS and PowerSource;
- restricting access to PowerSource's remote maintenance support feature with limited time that a user may access the SIS environments when using this feature;
- reducing the number of SIS environments that a single user may access during a 24-hour period;
- turning off the remote maintenance support for all PowerSchool customers who had the feature as "always on" and then removing the option to even select "always on";
- protecting endpoints and servers with endpoint detection and response (EDR) software that provides advanced security monitoring, threat detection, next-generation antivirus, and real-time EDR capabilities;
- implementing technical audits of all accesses made of data to validate and reinforce PowerSchool's security framework, including shortening the time-windows for authorized maintenance;
- protecting PowerSchool systems using a 24-7-365 threat hunting protection service; and
- configuring its systems and data storage with AES-256 encryption for data at rest.

[203] I asked the institutions and PowerSchool to provide me with a number of policies and reports (set out under the Technological and Security Safeguards section) and requested they highlight any changes they made, following the cyberattack.

---

[90] Planning for Success: Privacy Impact Assessment Guide | IPC.

[204] Despite my requests, PowerSchool only provided the IPC with a revised Security Incident Response Procedure where I note limited changes were made to the procedure after the cyberattack.

[205] PowerSchool has provided no evidence to the institutions or the IPC of any other changes to its security and information management policies and procedures. I find this very concerning particularly after an international cyberattack of this scale which revealed all the above-noted security issues in PowerSchool's SIS and PowerSource.

[206] I recommend the institutions review and require PowerSchool make changes to its security and information management polices and procedures, if and as needed, particularly regarding the early breach detection process, Access Control Policy, Third Party Management Policy, Asset Management Policy, Password Policy, Incident Response Policy, Monitoring Policy, Security Awareness & Training Policy and the Security Incident Response Procedure. Institutions should monitor and enforce implementation of those changes.

[207] Regarding my request for recent Audit Reports produced after the cyberattack, PowerSchool submitted that its SOC 2 Type 2 Audit Report was underway for 2025 and that the recertification process under ISO standard was on-going with no exact date of completion. In its November 12, 2025 submissions on a draft version of this report, PowerSchool advised that it had since completed a 2025 SOC 2 Type 2 audit and ISO recertification process, though no specific dates of completion were provided. It is also not clear whether these included PowerSource in its scope. PowerSchool submitted that these audit reports were posted to the named account, again with no specified date. PowerSchool indicated ongoing efforts to provide the institutions with current reports through the named account.

[208] In response to my request for recent PowerSchool's penetration testing and vulnerability risk assessment reports (collectively, the vulnerability assessments) showing that PowerSource and the SIS are in scope after the cyberattack, PowerSchool advised these vulnerability assessments are conducted as part of its normal operations. PowerSchool submitted that it is not necessary for the vulnerability assessments to be provided to the IPC in this investigation, taking the position that the vulnerability assessments are routine rather than remedial steps undertaken because of this cyberattack.

[209] Notably, even though all the institutions requested the 2025 vulnerability assessments,[91] PowerSchool did not provide these assessments to the affected institutions either. While I acknowledge that these types of vulnerability assessments contain confidential and sensitive information, it is important for the institutions to be able to confirm that both SIS and PowerSource are within the scope of these vulnerability

[91] As noted earlier in this investigation, PowerSchool only provided a Penetration Testing Summary Report dated June 25, 2024, which did not confirm PowerSource was within the scope for the period of April 30 to June 25, 2024, though SIS was in scope.

assessments conducted since the cyberattack. Further, it is important for the institutions to be knowledgeable of any major issues or potential vulnerabilities involving the personal information either held or accessible through SIS and PowerSource. As such, it is crucial that the institutions demand to receive these recent vulnerability assessments from PowerSchool.

[210] I recommend the institutions review the named account where PowerSchool committed to periodically posting updates and reports. If not posted by PowerSchool on the named account, the institutions should require PowerSchool provide them with a copies of its 2025 SOC 2 Type 2 audit report, ISO recertification standard report, and vulnerability assessments.

[211] Institutions should obtain this evidence from PowerSchool to ensure compliance with their obligations under the *Acts* and regulations to protect personal information in their custody or control. I strongly recommend the institutions not accept PowerSchool's assurances at face-value, but rather, hold PowerSchool accountable using the relevant provisions in the Agreements to require PowerSchool document and show compliance.

[212] I note on July 15, 2025, a Letter of Commitment was signed by PowerSchool with the OPC outlining PowerSchool's commitments to take additional actions involving certain security safeguards and measures to continue to address the cyberattack and to prevent future breaches.[92] PowerSchool will provide the OPC with information and evidence of additional actions it committed to undertake from July 2025 to March 2026.[93] Institutions should, in my view, insist on receiving this information as well.

Overall Conclusions Regarding Remedial Measures

[213] Throughout this investigation, I remain concerned that certain institutions still lacked the following measures: robust breach response plans and efficient early breach detection processes involving their service provider; clear retention schedules and processes for regularly purging personal information accordingly; and proper monitoring, evaluation and enforcement of privacy and security measures to protect personal information held in PowerSchool's SIS and PowerSource.

[214] I acknowledge that the institutions are working towards improvements within their organizations as well as with PowerSchool, however these efforts are inconsistent. I strongly recommend all institutions strengthen their own privacy and security practices as necessary. I also strongly recommend that the institutions hold PowerSchool accountable as their service provider to ensure that they – *the institutions* – comply with the *Acts* and their regulations. This requires institutions take active and prompt steps to work collaboratively with each other as a sector, and with PowerSchool, to implement the recommendations made in this report and follow up accordingly.

[92] Letter of Commitment to the OPC.
[93] Letter of Commitment to the OPC.

[215] Until this is done, I find the institutions have not responded adequately to the breach.

CONCLUSION:

Based on the results of my investigation, I have reached the following conclusions:

Technical and Security Safeguards

1. At the time of the cyberattack, the institutions, through their service provider PowerSchool, did not have reasonable security measures in place as required by section 3 of Regulation 823 under *MFIPPA* and section 4 of Regulation 460 under *FIPPA*. Many vulnerabilities contributed to a threat actor successfully exploiting PowerSchool's education technology, including the following:

    a. compromised credentials of a subcontractor with elevated privileges;

    b. failure to detect four months of unauthorized activities and the cyberattack in a timely manner due in part to limited log retention periods;

    c. lack of multi-factor authentication required for PowerSource; and

    d. failure to limit remote maintenance support access on an "as needed basis" only.

2. At the time of the cyberattack, some institutions were collecting highly sensitive personal information that was not necessary to fulfil their education mandate (including health information numbers, SINs, and insurance policy numbers). Also, some institutions were retaining personal information in their SIS far beyond reasonable retention periods, with some data going back as far as 60 years, failing to securely purge information in accordance with applicable retention periods. These poor information practices amplified the scope of the breach and the real risk of significant harm for impacted individuals.

3. At the time of the cyberattack, some institutions lacked a breach response plan or protocol that involved their service provider. More concerning is that one institution acknowledged not having a breach response plan at all.

Contractual Agreements and Oversight Measures

4. Certain institutions did not have reasonable provisions in their Agreements with PowerSchool to ensure the privacy and security of the personal information under their custody or control as required by section 3 of Regulation 823 under *MFIPPA* and section 4 of Regulation 460 under *FIPPA*. Certain Agreements:

a. were outdated, as far back as 2011;

b. lacked one or several IPC recommended provisions (confidential information, notice of compelled disclosure, subcontracting, security, retention and destruction, audits, and governing laws); and

c. did not incorporate reasonable retention schedules within the Agreements.

5. The institutions did not have sufficient oversight and monitoring measures in place with respect to PowerSchool at the time of the cyberattack to ensure the privacy and security of the personal information under their control, as required by section 3 of Regulation 823 under *MFIPPA* and section 4 of Regulation 460 under *FIPPA*. Specifically, the institutions:

    a. did not have a formal system in place to regularly monitor or oversee PowerSchool's compliance with the provisions set out in the Agreements; and

    b. failed to obtain documented evidence of PowerSchool's fulfillment of periodic or at least annual risk assessments, audits and compliance reports [ISO standard certification and/or recertification, and SOC 2 reports] confirming compliance with industry standards as required in many Agreements.

Given the above, I find the institutions did not have reasonable measures in place to prevent unauthorized access to personal information in accordance with the requirements of the Acts and their regulations, and did not, as a whole, respond adequately to the breach.

RECOMMENDATIONS:

I make the following recommendations to all the institutions to the extent they do not already comply with them, or have not already implemented them:

Technical and Security Safeguards

1. Limit access to their SIS through PowerSource, or any other remote maintenance support connection, for only as long as necessary to provide the requested technical service.

2. Review PowerSchool's security and information management policies and procedures and associated documentation to ensure they address identified vulnerabilities that contributed to the cyberattack in this case, including:

a. User access privileges, especially elevated access privileges for remote maintenance personnel;

b. multi-factor authentication requirements to access PowerSource; and

c. reasonable retention periods for network and security logs.

3. If the institution determines that changes are required, the institution should bring those to PowerSchool's attention and insist that PowerSchool implement those changes to the extent they are reasonable in the circumstances, consistent with the *Acts*, current industry standards, and best practices.

Contractual Agreements and Oversight Measures

4. Review and, as necessary, renegotiate Agreements with PowerSchool to incorporate the recommended contractual provisions to address the privacy and security of personal information, including ownership of data, collection, use and disclosure, confidential information, notice of compelled disclosure, subcontracting, security, retention and destruction, audits and governing laws.

5. Review and, as necessary, renegotiate Agreements with PowerSchool to include robust contract enforcement provisions to allow institutions to demand documented evidence from PowerSchool demonstrating its compliance with the terms and conditions of the Agreements.

6. If it is not possible to review and renegotiate the Agreements in a timely manner, the institutions should enter into an addendum to the Agreements with PowerSchool, until such time as the Agreements can be renewed or renegotiated.

7. Take steps to standardize, define and document the monitoring of security and auditing provisions under the Agreements and obtain evidence of PowerSchool's fulfillment of its contractual obligations on an annual basis. This includes effective monitoring of PowerSchool's security measures in compliance with legal requirements, current industry standards and best practices that are reasonable in the circumstances. Relevant evidence includes PowerSchool's annual ISO standard surveillance audit reports, ISO standard recertification audit report, SOC 2 Type 2 report, and penetration testing and vulnerability risk assessment reports in respect of PowerSchool's technological products, including SIS and PowerSource.

8. Take decisive action to enforce the relevant contractual provisions against PowerSchool, in the event PowerSchool does not comply with its contractual obligations to protect and secure personal information it processes on behalf of the institutions.

Other Recommendations

9. Immediately cease the collection of any personal information that is not necessary to fulfil their educational mandate, including students' health card numbers, social insurance numbers, and insurance policy numbers as such collection contravenes the *Acts*.

10. Review their data retention periods and develop their data retention schedules, if not already done, for any personal information contained in PowerSchool's SIS and PowerSource, including their own networks and securely destroy any data holdings that exceed such periods in accordance with the *Acts* and their regulations.

11. Review their privacy breach response plans or protocols, policies and practices to determine whether changes are needed in light of my findings in this report, particularly in respect of their relationship with service providers. In the case of the one institution that does not have such a breach response plan or protocol in place, create and implement one as soon as possible. Periodically, request PowerSchool's Security Incident Response Procedure to review it to confirm consistency with relevant industry standards that are reasonable in the circumstances to ensure compliance with their breach response obligations under the *Acts* and determine whether changes are needed, accordingly.

12. Take steps to ensure that all individuals whose personal information was involved in the cyberattack have been notified, if not already done, and going forward, any indirect notices should be prominently displayed on websites (or other communication channels or media sites) to improve public outreach.

13. Conduct PIAs on PowerSchool's SIS and PowerSource. The institutions subject to *FIPPA* are required to carry out PIAs. As a best practice, institutions subject to *MFIPPA* should also conduct PIAs. Use the IPC's updated *Planning for Success: Privacy Impact Assessment Guide*[94] which sets out step-by-step guidance on how to conduct a PIA from beginning to end.

14. When contracting with a service provider like PowerSchool for services involving an information or data management system, portal, or technology, institutions should ensure they carry out the appropriate due diligence to protect personal information in their custody or under their control throughout the entire procurement process -- from planning to tendering, vendor selection, contracting, agreement management, right up to and including termination. Institutions should follow the IPC's Guidance *Privacy and Access in Public Sector Contracting with Third Party Service Providers*[95] which includes best practices and recommendations to support the proper accountability of service providers who manage personal information on behalf of institutions.

---

[94] Planning for Success: Privacy Impact Assessment Guide | IPC.
[95] Privacy and Access in Public Sector Contracting with Third Party Service Providers | IPC.

Within six months of receiving this report, the institutions will separately provide the IPC with proof of compliance or the status of their efforts to comply with the above recommendations.

Original Signed by: November 17, 2025

Harpreet Bains
Investigator

COMMISSIONER'S MESSAGE TO THE SECTOR AS A WHOLE

I have thoroughly reviewed the above report and fully endorse the investigator's findings and recommendations.

This case is another stark reminder that while institutions may outsource some of their responsibilities to third party service providers, they cannot outsource their accountability for ensuring reasonable measures are in place to prevent unauthorized access to personal information in their custody or under their control.

To address the serious vulnerabilities identified in this report in a comprehensive and consistent manner and to effectively mitigate the chances of such a cyberattack recurring, I believe it will take a highly coordinated, sector-wide approach.

I therefore call on all Ontario school boards, both large and small, to work together when negotiating new or revised Agreements with ed tech providers to ensure inclusion of the IPC's recommended privacy and security provisions. By doing so, Ontario's school boards can also exact more leverage in requiring ed tech providers to provide them with the information and documentation necessary to effectively oversee and monitor compliance with the agreements.

I also call on the more sophisticated school boards with the requisite cybersecurity knowledge and expertise to share with others their analyses of audit reports, certification reports, penetration testing and vulnerability assessment reports of a given ed tech provider. Such cooperation among the boards would serve to alert one another of any identified risks so they can work in concert to demand prompt remedial action by the service provider, failure of which could result in serious consequences, including possible termination of all agreements with school boards across Ontario.

I call on the Ministry of Education and the Ministry of Public and Business Service Delivery and Procurement to support Ontario's school boards in these efforts by providing clear procurement parameters respecting the use of ed tech in schools. By bringing its leadership and influence to the table, the Ontario government can drive a more coordinated approach to contract negotiations and enforcement with ed tech companies.

I also urge the government to provide the necessary cybersecurity training, guidance and resources to school boards, and to leverage their capacity, as appropriate, to elevate the overall cyber resilience of the sector as a whole. Some of these measures could be achieved, in my view, by urgently adopting regulations under the *Enhanced Digital Security and Trust Act, 2024*, enacted as part of Bill 194 in 2024.

A sector-wide coordination and cooperation among school boards, strongly supported by government, would strengthen contract negotiations with ed tech providers, as well as the oversight and monitoring measures necessary to ensure institutions' compliance with their obligations under the *Acts*.

Most importantly, such efforts would provide Ontario students, their parents and guardians, and educators with the personal information protection they deserve and an education system they can trust.

Original Signed by: November 17, 2025

Patricia Kosseim
Commissioner