Office of the Information and
Privacy Commissioner of Alberta

Investigation Report F2025-IR-02

Investigation into the PowerSchool Breach

November 17, 2025

Schools, School Boards, Francophone Regional Authority

1. Calgary Board of Education
2. Calgary Arts Academy Society
3. Foundations for the Future Charter Academy
4. Living Waters Catholic Separate School Division
5. STEM Innovation Academy
6. Wild Rose School Division
7. Red Deer School Division
8. Sturgeon Public School Division
9. Grande Prairie Roman Catholic Separate School Division
10. Fort Vermilion School Division
11. Red Deer Catholic Separate School Division
12. Southern Francophone Education Region
13. Peace River School Division
14. Horizon School Division
15. Wolf Creek School Division
16. Clearview School Division
17. Medicine Hat School Division
18. Lakeland Roman Catholic Separate School Division
19. Fort McMurray Public School Division
20. Alberta Classical Academy
21. Livingstone Range School Division
22. Thrive Charter School Society
23. Holy Spirit Catholic School Division
24. East Central Catholic Schools
25. STEM Collegiate Canada Society
26. Medicine Hat Catholic Board of Education
27. Buffalo Trail Public Schools
28. Rocky View Schools
29. Elk Island Catholic Separate School Division
30. Grande Yellowhead Public School Division
31. Peace Wapiti Public School Division
32. Connect Charter School Society
33. Battle River School Division

Table of Contents

Investigation Report Summary

Between January and April of 2025, 33 public and charter schools, school boards and a Francophone regional authority (collectively referred to as "Educational Bodies") in Alberta[1] reported to my Office that their service provider, PowerSchool Canada ULC[2] (PowerSchool), had experienced a cybersecurity incident (Incident) that had resulted in the compromise of personal information stored in their respective instances of the Student Information System (SIS). PowerSchool also submitted information to my Office regarding the Incident. PowerSchool reported that a threat actor gained access to the SISs using a compromised (stolen) set of credentials belonging to a support staff. The threat actor used the stolen credentials to first gain access to PowerSchool's community-focused customer support portal PowerSource. From PowerSource, the threat actor then gained access to the SISs using the same set of credentials. It was reported by these Educational Bodies that personal information of students, parents/guardians and staff were involved in the Incident. Among the personal information compromised from the SISs was:

- for students - names, student ID numbers, gender, date of birth, home addresses and phone numbers, custodial agreements, medical information, Personal Health Number (PHN);
- for staff - home address and phone numbers, employee numbers and email addresses and in some cases social insurance numbers; and
- for parents/guardians - home address and phone numbers, work and other phone numbers, email addresses, and as applicable, custodial arrangements.

These Educational Bodies are public bodies under the *Freedom of Information and Protection of Privacy Act* (FOIP Act or Act). As public bodies under that Act, they are obligated to comply with the privacy provisions therein, including for the protection of personal information from unauthorized access and disclosure.

Over 700,000 individuals were affected by the PowerSchool Incident in Alberta. Given the magnitude of this breach and the sensitivity of personal information involved, particularly as it relates to the students, I decided to initiate an investigation on my own motion under section 53(1)(a) of the FOIP Act. This section allows me to conduct investigations to ensure compliance with any provision of the Act.

The investigation initially was informal. However, as my team and I worked through the investigation and analyzed the evidence, I decided to move it to a formal investigation. My investigation examined whether the Educational Bodies made reasonable security arrangements to protect the personal information involved in the Incident pursuant to section 38 of the FOIP Act. This section requires public bodies to "make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction".

My investigation found that the Educational Bodies did not meet their security obligations under section 38 of the FOIP Act for the following reasons.

[1] As listed on the cover page of this Investigation Report.

[2] "ULC" means an unlimited liability corporation.

- They did not have policies or procedures, as required by section 38, to facilitate their compliance with their respective section 38 obligations including for vendor management.
- There were significant gaps in PowerSchool's security measures which contributed to the breach of the personal information of the students, parents/guardians and staff. The measures were found to fall below the standard required by section 38 as it relates to the Incident. Given this, and because these public bodies are accountable for the actions or inaction, as the case may be, of PowerSchool, I found that these public bodies did not meet the requirements of section 38 because of these gaps as it relates to the Incident.

To remedy the non-compliance that I have found, I made 22 recommendations in total, including six to the Educational Bodies, thirteen to PowerSchool, and three to Government. They focus on remedying the non-compliance found and preventing future breaches of personal information involving technology used by the Educational Bodies.

Methodology

I initiated the investigation on January 9, 2025. I assigned a Senior Information and Privacy Manager in my Office to assist me in conducting the investigation. Initially the investigation was informal. However, given what we discovered on analyzing the evidence gathered and the magnitude of the breach, I decided to conduct a formal investigation.

In March of 2025, I notified each of the Educational Bodies about the investigation in a letter. Therein, they were asked to provide us with any contracts they had signed with PowerSchool concerning the service PowerSchool provided to them that involved the collection, use and disclosure of personal information. They were also asked to provide us with the following information:

1. any information about security arrangements and retention concerning the personal information stored in the SIS;
2. details concerning what personal information was stored in their instances of the SIS;
3. any security and retention policies and procedures concerning the personal information involved in the Incident;
4. details concerning whether the personal information was held on premises or in the cloud; and
5. information concerning how and when the Incident was learned about and steps taken after the Incident, including containment and mitigations.

From the breach reports submitted to my Office by the Educational Bodies, we were able to identify the number of affected individuals and the types of personal information involved.

On January 10, 2025, my Office received a preliminary and informal notification about the Incident from PowerSchool's legal counsel. On May 30, 2025, PowerSchool received a letter wherein we asked them a series of questions related to the Incident. PowerSchool provided responses to the questions in a letter dated July 11, 2025. Included with the letter were five documents:

1. PowerSchool – PowerSchool SIS, ed-Fi/DE and… Summary Report, dated June 25, 2024, on a crowd-source penetration test conducted by a third party

2. Decommission Policy, dated April 1, 2025
3. Information Security Policy 001, Information Security Management System (ISMS) Governance Policy, undated
4. Network Security Diagram
5. PowerSchool Group LLC, SOC 2, Type 2 2024
6. Report on PowerSchool Group LLC's description of its system and on the suitability of the design and operating effectiveness of its controls relevant to security, availability, and confidentiality, pursuant to reporting on system and organization controls 2 (SOC 2) Type 2 examination performed under AT-c 105 and AT-c 205, July 1, 2023, to June 30, 2024

We reviewed the Investigation Report prepared for PowerSchool by Crowdstrike, dated February 28, 2025, which was also provided to us by PowerSchool.

On October 27, 2025, in a letter I notified the Educational Bodies and PowerSchool about the investigation moving to a formal investigation and provided a copy of the Preliminary Investigation Report as it was drafted at that time. We invited each of the Educational Bodies and PowerSchool to provide representations on the content. We considered the representations received and have incorporated any that are relevant to the issue and the findings related to the same into this Investigation Report.

Explanatory Note

All section references used in this Investigation Report are to the FOIP Act unless otherwise stated.

For clarity, the findings and recommendations contained in this Investigation Report apply to those Educational Bodies that reported the Incident to my Office as listed on page 1. However, for any public and charter schools, and school boards or any other educational body that were public bodies under the FOIP Act, and that did not report the PowerSchool breach to our office having been involved in the same (not a mandatory requirement under that Act), the recommendations should be considered as applicable to these bodies.

Background

PowerSchool software

[1] PowerSchool's software offers an integrated suite of tools to assist schools to manage student information, enable personalized learning, support educators, and streamline administrative operations. Among the suite of tools is the Student Information System (SIS), which helps schools manage student enrollment, personal and medical information, attendance, and academic data. Each of the Educational Bodies involved in this investigation used this software for varied purposes.

[2] PowerSchool offers the SIS as both an on-premises and cloud-hosted solution. Customers that elect to use PowerSchool SIS on-premises install the product on their own servers, configure the product, and hold responsibility for managing the product's deployment and data. Customers who select the cloud-hosted option have their PowerSchool SIS data stored in a cloud-hosted environment managed by PowerSchool. Four of the Educational Bodies' implementation of SIS was on-premises. One of the school board's implementation of the SIS was in the cloud managed by the school board, not PowerSchool. The rest had their instances of the SIS in the cloud hosted by PowerSchool.

The Cybersecurity Incident

[3] On December 28, 2024, PowerSchool discovered that it was the victim of a cyberattack. The attack led to unauthorized access and exfiltration of personal information from PowerSchool's SISs through one of its community-focused customer support portals, PowerSource. PowerSchool reported that the Incident occurred between December 19 and 28, 2024. PowerSchool notified the affected Educational Bodies about the breach, and the Incident was reported to my Office by these bodies between January and April of 2025. The Educational Bodies reported to my Office that they were notified about the breach by PowerSchool on January 7, 2025.

[4] Based on the Crowdstrike investigation report, the objectives of Crowdstrike's investigation into the Incident were to determine:

- how the threat actor gained access to the PowerSchool environment;
- the earliest and most recent dates of threat actor activity;
- whether the threat actor moved laterally in the PowerSchool environment and, if so, how;
- whether there was any evidence that the threat actor accessed or exfiltrated PowerSchool data and, if so, what data was accessed or exfiltrated; and
- whether the threat actor persists in the PowerSchool environment, or whether they have been evicted.

[5] In the Crowdstrike report, the Incident was described as follows.

- The threat actor gained access to the PowerSchool environment on December 19, 2024.
- The threat actor performed "Maintenance Remote Support" operations in PowerSource using the compromised support credentials, which enabled the threat actor to access the individual customer organizations' SIS instances.
- The threat actor exfiltrated the data from the Teachers and Students tables of the SIS.
- Beginning on August 16, 2024, at 01:27:29 UTC, PowerSource logs showed that an unknown actor successfully accessed the PowerSchool PowerSource portal using the compromised support staff credentials. CrowdStrike 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.

- The most recent evidence showed that the threat actor used the compromised credentials to log into the maintenance interface of PowerSource to interact with the SIS.[3]

[6] The credentials used by the threat actor were those of a PowerSchool contractor, whose credentials had been compromised. The contractor had administrative level privileges, which enabled the contractor to perform IT functions, including maintenance of the PowerSchool systems, including the SIS. According to the Crowdstrike report, "PowerSource allows a support technician with sufficient permissions to gain access to customer SIS database instances for maintenance purposes."

[7] The personal information involved in the Incident as reported by the Educational Bodies varied among them, but generally included names, telephone numbers, dates of birth, genders, grades, school-issued email addresses, Alberta student ID numbers, and school-issued ID numbers of students. Medical information consisting of allergies, medication, medical conditions, Personal Health Numbers (PHNs), physician contact information and guardian information were also compromised. For staff of the Educational Bodies (e.g. teachers), employment information including income, years at current job, names, mailing address, email address and internal identification number were also compromised. Some reported the inclusion of social insurance numbers. Information of parents/guardians included in students' records was also compromised, including home addresses and phone numbers, work and other phone numbers, email addresses, and, as applicable, custodial arrangements (collectively, the Personal Information).

[8] In its representations to the Preliminary Investigation report, PowerSchool indicated that the scope of the data breach was more limited than was reported by the Educational Bodies. On this point, it stated:

> *Data Involved. The Draft Report states, "[i]t was reported by these Educational Bodies that personal information of students, parents/guardians and staff were involved in the Incident" describes the categories of information allegedly compromised. As stated in the publicly available CrowdStrike Report, the threat actor exfiltrated data only from the Student and Teacher tables for certain customers. There is no evidence of exfiltration from other SIS tables. There were no separate parent/guardian tables exfiltrated.*
>
> *Student/Teacher Table Fields. Student table fields commonly included names, student IDs, gender, date of birth, addresses, phone numbers, limited medical alert notes, and parent/guardian names. Teacher table fields commonly included names, addresses, phone numbers, employee numbers, and email addresses. The tables did not include fields for Personal Health Numbers (PHNs), custodial agreements, teacher income, or staff "years at current job." Moreover, each school decides what data they wish to input into the SIS, and the information involved varies across school systems.*

[3] At pp. 5 and 6.

> *Medical Alert Field. The "alert_medical" field is a limited free-text field intended for concise alerts (e.g., "peanut allergy," "see nurse," or "asthma"). The field did not call for, and in the observed instances did not contain, detailed medical information of students. In the vast majority of instances, this field was unused or contained entries such as "none" or "N/A."*

[9] It added "[in] light of the above, PowerSchool requests revisions to the "Investigation Report Summary" to reflect the above factual scope, adding further "PowerSchool disagrees with the assertion in [a] paragraph that "[t]his information, particularly the medical information, is highly sensitive".

[10] The scope of the personal information involved in the breach, as described above, was gathered directly from the Educational Bodies. In response to our question to each of them about the personal information involved in the breach, each provided a listing. Examples of the detail provided are set out below.

- *Students: first, middle and surname,* [Educational Body] *student ID#, gender, date of birth, grade, school,* [Educational Body] *issued email address, home address, home phone number, guardian alert (text field), medical alert (text field). Guardian alert field holds notations such as "court order, custody agreement, etc. without containing the actual information. The medical alert field contains medical information such as allergies, diagnosis, medication and treatments, accommodations required. Of the total 593,517 student records, 105,884 contained information in the medical alert field and 15,564 contained information in the guardian alert field. Staff: First, middle and surname,* [Educational Body] *employee#, school name, address and phone number,* [Educational Body] *issued email addresses. Of the 28,156 staff, 113 had information in the home phone number field and 51 had information in the home address field*

- *Student tables including: student full name, address, birthdate, home phone, entry/exit enrolment info, grade level, ASN, medical alerts, legal alerts (guardianship). A full list of data that is stored in our students tables is attached to this report. Teacher tables including: first name, last name, email address.138 Students with medical alerts. 5 Students with legal alerts*

- *Student (Current & Past Students of our School Division): Legal Names, Preferred Names, Mailing Addresses, Dates of Birth, Home Phone Numbers, Health Care Numbers, Basic Medical Conditions (Asthma, diabetes, allergies), Gender, Photo of Student, Self Identified as Indigenous, Treaty Numbers, Locker information, Citizenship Information (Birth Certificate, Passport, Study Permits), Court Orders/Parenting Orders, Academic Records, Log Entries, Incident Reports, Attendance, Academic Records, Associated Family Members, Contacts, School Enrollments, Student Email Address. Contacts (Caregivers, Emergency Contacts): Relationship to Student, First and Last Name, Email Address, Phone Numbers, Address. Teachers/Admins/Librarians/Secretaries: First and Last Name, Work Email, Gender, Teacher ID Number, Some Home Addresses and Personal Phone Numbers.*

- *Information on Students which included: Name, mailing address, physical address, date of birth, email, phone number. Information on Parents/Guardians included: Names, addresses, phone numbers, email addresses. Staff information Included: staff name and email address.*

[11] Despite PowerSchool's views on the information breached, it is clear based on the submissions of the Educational Bodies that a wide array of personal information was involved in the breach, and I accept the same as fact. Perhaps there is some misunderstanding as to how the data fields in the tables are to be filled out by PowerSchool customers which has led to this discrepancy between PowerSchool's views and how these tables are being populated. This issue must be addressed between PowerSchool and the Educational Bodies because it is the sensitivity of the combined personal information stored in PowerSchool's databases that sets the standard for security arrangements under section 38.

[12] In terms of PowerSchool's views on the sensitivity of the personal information involved, I disagree with its views that the personal information, taken together, is not highly sensitive. As can be seen from the personal information involved in the breach as reported by the Educational Bodies, it is clearly highly sensitive. I would add here that in the Protection of Privacy (Ministerial) Regulation, which now applies to these Educational Bodies, personal information respecting a minor is deemed to be of high sensitivity[4]. Although this Regulation was not applicable at the time of the Incident, the definition of high sensitivity personal information therein, particularly about children, is informative.

Application of the FOIP Act

[13] The FOIP Act applies to an "educational body" as described in section 1(d). "Educational body" is included in the definition of a "local public body" under section 1(j). Local public bodies are "public bodies" under the Act pursuant section 1(p). The 33 Educational Bodies that reported the incident to my Office are public bodies that are subject to the FOIP Act.

[14] Section 4(1) states that the "Act applies to all records in the custody or under the control of a public body …"

[15] A service provider under contract to a public body is considered an "employee" of the public body.[5] The public body is responsible for compliance with the Act for its employees:

> *1 (e) "employee", in relation to a public body, includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body;*

[16] PowerSchool's services were provided to the Educational Bodies under contract. As such, I find that for the purposes of the FOIP Act, PowerSchool is an employee of each of the Educational Bodies. As an employee, each of the Educational Bodies is accountable for PowerSchool's compliance with the FOIP Act.

[4] Alberta Regulation 143/2025.

[5] Section 1(e).

[17] In its representations to the Preliminary Investigation report, PowerSchool took issue with this finding. It stated:

> *The Draft Report concludes that PowerSchool is an "employee" of each Educational Body for FOIP Act purposes. PowerSchool respectfully disagrees with that characterization and requests that findings predicated on that conclusion be revised. PowerSchool provides services under contract and does not accept the "employee" designation.*

[18] As set out above, the scheme in the FOIP Act includes the definition of employee, which includes "a person who performs a service for the public body…under a contract…with the public body". Section 28(1)(nn) of Alberta's *Interpretation Act* clarifies that "in an enactment, "person" includes a corporation". PowerSchool is a corporation, and it performs services for the Educational Bodies under a contract. As such, it is an "employee" of the Educational Bodies *for the purposes of that Act.* The purpose of defining employee this way is to ensure that the FOIP Act remains applicable to any contracted services provided to public bodies by third party service providers. Any other interpretation would result in an absurdity such that by simply outsourcing services, public bodies could avoid application of the FOIP Act.

Section 38 Duty to Protect Personal Information

[19] Section 38 sets out a public body's obligations for the protection of personal information in the custody or control of the public body. It states:

> ***38*** *The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.*

[20] This section requires a public body to protect personal information by making reasonable security arrangements appropriate to the sensitivity of the personal information.[6] Extremely sensitive personal information, such as medical information, requires more stringent protection arrangements.[7] It also requires that public bodies implement physical, administrative and technical controls[8] to ensure this protection[9]. It is also essential for a public body to implement a breach management and response protocol within its security framework.[10]

[6] Annotated FOIP Act at p. 5-38-1, citing F2018-IR-03.

[7] Annotated FOIP, at p. 5-38-1.

[8] Administrative controls include a governance framework inclusive of policies and procedures designed to protect personal information. Physical controls protect physical assets containing personal information. Technical controls are technical measures employed to protect electronic personal information and to control access.

[9] From p. 5-38-1, citing Orders F2014-19, F2022-23 and F2022-54 (see p. 5-38-54) of Annotated FOIP "The Office of the Information and Privacy Commissioner has consistently urged organizations to implement three layers of protection: physical, administrative and technical/electronic (e.g. PIPA Advisory 8: Implementing Reasonable Safeguards", and Investigation Reports P2006-IR-005, H2006-IR-002, H2007-IR-002). While these requirements have been raised in investigations conducted under the *Personal Information Protection Act* (PIPA) and the *Health Information Act* (HIA) these requirements are also relevant to public bodies subject to the FOIP Act (Investigation Report F2013-IR-01 [24]).

[10] Annotated FOIP Act at p. 5-38-1, citing F2018-IR-03.

[21] Taking reasonable measures to protect against risks implies that there is a need to identify and analyze what kinds of risks may affect personal and health information.[11] "Reasonableness" does not mean perfect.[12]

[22] In a joint publication, my Office together with the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of British Columbia set out what is needed to meet the reasonable standard for securing personal information under both private sector and public sector privacy legislation in Canada, including the FOIP Act. In the document "Securing personal information: A self-assessment for public bodies and organizations" it was identified that reasonable safeguards include several layers of security, including:

- risk management;
- written privacy and security policies;
- human resources security;
- physical security;
- technical security;
- incident management; and
- business continuity/disaster recovery planning.[13]

[23] It was also identified that the reasonableness of security measures adopted by an organization must be evaluated considering a number of factors including:

- the sensitivity of the personal information;
- the foreseeable risks;
- the likelihood of damage occurring;
- the medium and format of the record containing the personal information;
- the potential harm that could be caused by an incident; and
- industry standards.[14]

[24] It was also noted in the document that "[g]enerally accepted or common practices in a particular sector may be relevant to the reasonableness of a security safeguard. However, you must complement generally accepted practices and technical standards by elementary caution and common sense. In a digital world, it is more important than ever that organizations and public bodies maintain public trust by making all reasonable efforts to avoid a breach."[15]

[25] In the document "Contract Managers Guide to Freedom of Information and Protection of Privacy and Records Management in the Government of Alberta" published by the Government of Alberta, it specifies that there are considerations that must be taken into account by public bodies when entering into a contract with service providers, or other third parties, wherein the service provider will have access to personal information of the public body. The guidance specifies that

[11] *Ibid.*, citing Investigation Reports F6336, P2137, H4943 and H4944.
[12] *Ibid.,* citing F2016-IR-02.
[13] At p. 2.
[14] *Ibid.*
[15] At p. 3.

contracts with service providers must contain certain provisions to ensure that the duties of the public body under the FOIP Act, as it relates to any personal information involved in the contract, will be met, namely provisions that:

- clarify that control of the personal information remains with the public body and that the FOIP Act applies to the information;
- specify how the public body maintains control, such as by setting out strict parameters of access, collection, use or disclosure of the personal information and, among other things, the duty to protect the information as required by section 38 including its retention and destruction;
- clarify that the contractor may only access, collect, use or disclose the personal information in accordance with the public body's duties under Part 2[16] of the FOIP Act as specified in the contract;
- specify that the contractor has policies and procedures sufficient to meet the public body's duties under the FOIP Act as it relates to the processing of any personal information under the contract, including for the protection of personal information and, in the absence of such policies or procedures, specify that the contractor is bound by the public body's policies and procedures as applicable thereto;
- specify what the contractor is to do in the event of a breach of the contract or of personal information, including the duty to report the same to the public body and the timing of the same;
- clarify what happens to the personal information on termination, which must either be returned to the public body or securely destroyed with the permission of the public body and that the contractor must not retain a copy of the personal information;
- allow the public body to audit for compliance with the contract; and
- stipulate that the contractor is accepting the same responsibilities to protect privacy as required under Part 2 of the FOIP Act.

[26] The FOIP Act was repealed on June 11, 2025. However, because it was in effect at the time of the Incident, this Act applies to the Personal Information involved in the Incident. The privacy Part in the FOIP Act was replaced with the *Protection of Privacy Act* (POPA) the same day it was repealed. This Act now applies to personal information in the custody or control of the Educational Bodies, including that stored in their respective SIS instances. How this Act factors into this investigation is discussed later in this Investigation Report.

[16] These are the privacy provision of the Act.

Issues for Investigation

[27] There is one issue for this investigation:

Did the Educational Bodies meet their respective obligations under section 38 of the FOIP Act as it relates to the protection of the Personal Information involved in the Incident?

Analysis

[28] Section 38 of the FOIP Act requires public bodies to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction. As part of this duty, a public body must have adequate policies and procedures in place to meet its section 38 obligations.

[29] When engaging a service provider to provide services that will involve the sharing of personal information with the service provider necessary to perform the services, the public body must have policies and procedures in place to ensure that the service provider will meet the public body's obligations under section 38. When engaging a service provider, this duty will generally involve assessing the service provider's security measures and practices to ensure they meet the public body's section 38 requirements and assessing these measures and practices against the public body's policies and procedures to ensure that the service provider's security measures and practices align with the same. It will also involve monitoring these measures and practices over time to ensure they continue to align.

Did the Educational Bodies have adequate policies and procedures in place to meet their section 38 obligations with respect to the protection of the Personal Information involved in the Incident?

[30] In our questions sent to the Educational Bodies, we asked each of them to provide us with information about any security and retention policies and procedures they had concerning the Personal Information involved in the Incident and about how they each managed the breach on learning of the Incident. We also asked them about any of PowerSchool's security arrangements and retention concerning the Personal Information.

[31] A summary of the responses we received is as follows.

- Many responded by pointing to the contract provisions with PowerSchool in response to our questions about PowerSchool's security and retention policies.
- A few Educational Bodies mentioned they had policies or procedures but did not provide them.
- Of the policies provided, most did not have clauses mentioning contractor provisions or how to deal with service providers. One policy from a school division that was quite fulsome had an information security policy that required that if the information from the school division was hosted by a service provider, the agreement must specify the privacy and security measures to be employed to ensure that the service provider provides the level of protection equivalent to that provided by the school division itself.

- Some described how they responded to the Incident without identifying any policy or procedure to guide the response and management.
- Four did not respond to our questions. A few submissions we could not open.

[32] Based on the foregoing, I conclude that the majority of the Educational Bodies that reported the Incident to us did not have adequate policies and procedures in place to meet their duties under section 38. The general lack of policies and procedures by some Educational Bodies to ensure compliance with the FOIP Act is concerning. I observe that without these policies and procedures, the privacy rights of students, staff and parents/guardians as codified in the FOIP Act will not be protected. Privacy does not happen on its own, it requires a concerted effort by public bodies to administer the law in such a manner to ensure these rights are protected, which includes creating and implementing policies and procedures that will ensure the public body meets its duties under the FOIP Act.

Educational Bodies' Representations to the Preliminary Investigation Report

[33] One Educational Body stated "[t]he report defines "reasonableness" as not requiring perfection but later appears to apply stricter expectations when assessing the breach" and adds "[p]erhaps this inconsistency could be highlighted, and could the Commissioner evaluate Boards' actions based on the stared [sic] "reasonableness" standards as opposed to perfection clarity that hindsight affords".

[34] As indicated above, what is reasonable depends on evaluating the sensitivity of the personal information, which determines the level of security to be applied to protect the information. Here, the personal information involved in the breach was highly sensitive. This fact establishes that the security measures required to meet the standard in this context must be advanced and proportionate to the sensitivity of the information. This standard was used to assess whether the Educational Bodies had adequate policies and procedures in place, which is a necessary security measure required to protect highly sensitive personal information. Among these policies and procedures must be vendor management policies and procedures, which must include evaluating the security practices of a vendor and auditing them from time to time to ensure the level of protection remains "reasonable". My evaluation of the policies and procedures provided by the Educational Bodies demonstrated that the majority did not have policies and procedures that meet this standard.

As an employee of the Educational Bodies, did PowerSchool have adequate administrative and technical measures[17] in place to ensure the Educational Bodies met their respective section 38 requirements in the FOIP Act?

[35] As indicated, all 33 Educational Bodies entered into an agreement with PowerSchool for it to provide the software services. Most Educational Bodies submitted that they relied on the security provisions set forth by PowerSchool in the agreements as sufficient to meet their respective section 38 requirements.

[17] Physical security measures are not at issue in this investigation.

Agreements with the Educational Bodies

[36] The versions of the agreements entered into by the Educational Bodies with PowerSchool, as provided to us by the Educational Bodies, are set out below.

2024	Master Services Agreement (2024 MSA)
	Global Data Privacy Agreement (2024 DPA)
	2024 DPA Schedule 1-B – Physical, Administrative, and Technological Safeguards (2024 Safeguards)
2022	Master Services Agreement (2022 MSA)
	2022 MSA Exhibit C - Data Privacy Agreement (2022 DPA)
	2022 DPA Schedule 1-C – Physical, Administrative, and Technological Safeguards (2022 Safeguards)
2021	Master Services Agreement (2021 MSA)
	2021 MSA Exhibit D– Data Privacy and Security (2021 DPS)
2020	Master Services Agreement (2020 MSA)
	2020 MSA Exhibit D – Data, Privacy and Security (2020 DPS)
2019	2019 Privacy Statement (one school)
2017	Licensed Product and Services Agreement (one school board)

[37] The Personal Information that was stored by PowerSchool under these agreements includes the information of children including their names, dates of birth, address and phone information, medical conditions, and PHNs, as well as for staff, their income. This information, particularly the medical information, is highly sensitive. As indicated above, what will be reasonable for the purposes of section 38 is based on the sensitivity of the combined information. Here the Personal Information that was stored by PowerSchool includes highly sensitive information. This means that the standard of security necessary to protect this information must be commensurate with the risk, thereby requiring PowerSchool to have advanced security measures in place.

[38] The majority of the Educational Bodies had entered into the 2024 MSA, 2022 MSA, 2021 MSA or the 2020 MSA. Therefore, it will be these versions that will be referred to in this analysis. Each of these MSAs include either a DPA or exhibits (DPSs) setting out PowerSchool's privacy and security framework.

[39] In each of the DPAs or DPSs, PowerSchool set out its security standards for protecting personal information processed using its software.

2024 (clause 4) and 2022 (clause 4) DPAs:

> *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, PowerSchool shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.*

2021 (clause 1.5) and 2020 (clause 1.6) DPSs:

> *PowerSchool will safeguard and keep confidential personal or sensitive information obtained from the User(s), including, but not limited to, personally identifying information such as the name, email address or screen name of the User(s).*

[40] In the Safeguard schedules to the 2024 and 2022 DPAs, PowerSchool details how it will secure the personal information.

> *A.1 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 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.1.6 Security Coordinator. PowerSchool will provide the name and contact information of PowerSchool's security coordinator for the Customer Data received pursuant to the MSA and this DPA upon written request.*
> >
> > *A.1.7 Vendor-Data Subprocessors Bound. PowerSchool will enter into written agreements whereby Vendor-Data Subprocessors agree to secure and protect Customer Data in a manner consistent with the terms of this exhibit and the DPA. PowerSchool will periodically conduct or review compliance monitoring and assessments of Vendor-Data Subprocessors to determine their compliance with this exhibit and DPA.*
> >
> > *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.1.9 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.

A.1.10 Audits and Compliance Reports. PowerSchool's security compliance is assessed by independent third party auditors. Upon Customer agreeing to an NOA, PowerSchool shall provide 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.

[41] Included in this schedule is PowerSchool’s Data Security and Privacy Plan, which states as follows.

(a) In order to comply with all Applicable Laws as related to data security and privacy requirements, PowerSchool follows its Data Security and Privacy Plan (“DSPP”) and will: Review its data security and global privacy statement and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this DSPP. In the event PowerSchool's policy and practices are not in conformance, PowerSchool will implement commercially reasonable efforts to ensure such compliance.

(b) *As required by the ISO 27001:2022* [in the 2024 DPA or the NIST Cybersecurity Framework in the 2022 DSP]*, in order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Agreement, PowerSchool will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Agreement:*

Data Security:

- *Data-at-rest & data-in-transit (motion) are encrypted*
- *Data leak protections are implemented*

Information Protection Processes and Procedures

- *Data destruction is performed according to contract and agreements [in 2022 DPS only]*
- *A plan for vulnerability management is developed and implemented Protective Technology*
- *A plan for vulnerability management is developed and implemented with protective technology*
- *Log/audit records are ascertained, implemented, documented, and reviewed according to policy*
- *Network communications are protected*

Identity Management, Authentication and Access Control:

- *Credentials and identities are issued, verified, managed, audited, and revoked, as applicable, for authorized devices, processes, and users*

> - *Remote access managed*
>
> *PowerSchool also conforms to the ISO 27001:2022 standard.*
>
> *(c) For any of its employees (or employees of any of its subcontractors or assignees) who have access to Protected Data, PowerSchool has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, PowerSchool will require that all of its employees (or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.*
>
> *(d) In the event that PowerSchool engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Agreement, it will require such subcontractors, assignees, or other authorized agents to execute written agreements requiring those parties to protect the confidentiality and security of Protected Data under applicable privacy laws.*
>
> *(e) PowerSchool will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and PowerSchool will provide prompt notification of any breaches or unauthorized disclosures of Protected Data. More information on how incidents are handled can be found in the Main Service Agreement ("MSA").*

[42] In each of the 2021 and 2020 DPSs, PowerSchool details how it will secure the personal information:

> ***3. Data Security.*** *PowerSchool agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices for digital storage of sensitive personal 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:*
>
> ***3.1.*** *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 Agreement,* [remainder only in the 2021 DPS] *and only on terms consistent or exceeding the data security measures required by this Agreement between the Parties.*
>
> ***3.2.*** *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 this Agreement in a secure digital environment and will not copy, reproduce, or transmit data obtained pursuant to this Agreement, except as necessary to fulfill the purpose of data requests by Customer.*
>
> ***3.3.*** *Employee Training. PowerSchool will provide periodic security training to those of its 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.*

> ***3.4.*** *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 this Agreement in an environment using a firewall that is updated according to industry standards.*
>
> ***3.5.*** *Security* ***Coordinator****. PowerSchool will provide the name and contact information of PowerSchool's security coordinator for the Customer Data received pursuant to this Agreement upon written request.*
>
> ***3.6.*** *Sub-processors Bound. PowerSchool will enter into written agreements whereby sub-processors agree to secure and* ***protect*** *Customer Data in a manner consistent with the terms of this* ***Section 3.*** *PowerSchool will periodically conduct or review compliance monitoring and assessments of sub-processors to determine their compliance with this* ***Section 3.*** *For the purposes of this Agreement, the term "sub-processor" means a party other than Customer or PowerSchool, whom PowerSchool uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to Customer Data* [“Customer Data” is replaced with “Personnel Data” in the 2020 DPS].
>
> ***3.7.*** *Periodic* ***Risk*** *Assessment. PowerSchool further acknowledges and agrees to conduct digital and physical periodic risk assessments at least annually and remediate any identified security and privacy vulnerabilities in a timely manner.*
>
> [Next section in the 2021 DPS only]
> ***3.8.*** *PowerSchool will follow its established access security policies to support the physical security of the Customer* ***Data*** *against such risks as unauthorized access, collection , use, disclosure or disposal, loss or modification. Such security arrangements will include, without limitation, reasonable technical, physical, and administrative safeguards.*
> [Bolding in original]

[43] Each of the MSAs, DPAs, and/or DPSs also address:

- Breach management and reporting, which, generally, requires PowerSchool to investigate the cause, mitigate the risks of harm to any individual, notify the customer without delay, and within 72 hours where access is by a third party, and in accordance with applicable law, provide the customer with information for notification of affected individuals, cooperate with the customer in investigating the breach, and provide the types of personal information involved in the breach and details associated with the incident and any information to facilitate notification as may be required by the customer. PowerSchool also indicates therein that it maintains a written incident response plan that is consistent with industry standards and the applicable law relevant to the incident.

- Termination and return or destruction of personal information, which, generally, requires PowerSchool to return or delete the personal information on written request by the customer. There are provisions to facilitate transfer as an alternative and partial deletion or destruction. It is included in these DPAs and DPSs that PowerSchool will not retain the information beyond the necessary period for disposition and will notify the customer when all the personal information has been returned/disposed/deleted.

[44] Taking into account the sensitivity of the Personal Information processed by PowerSchool and what is required in this case for the security to be 'reasonable', and considering what is said in the agreements, on the face of it, it appears that PowerSchool had reasonable security safeguards that would meet the requirements of section 38. This is because in the MSAs, DPAs, and DPSs, its measures include security governance, risk management procedures, risk assessments, password and credentials management, access controls based on need to know, written privacy and security policies, physical and technical security measures, incident management, training requirements, server authentication and data encryption, logging and auditing and associated procedures including third party auditing of its security controls, downstream sub-processor management, alignment with internationally-recognized information security standards, and procedures for return or destruction of the personal information on termination of the contract. These measures, if properly implemented by PowerSchool, would, in my view, enable the Educational Bodies to meet their respective duties under section 38 regarding the personal information contained in their respective instances of SIS.

[45] Given this, it is reasonable that the Educational Bodies would have relied on the security measures set out in the agreement as sufficient to meet their section 38 requirements. That said, it is these Educational Bodies that must meet the section 38 requirements and that are accountable for PowerSchool doing the same. The accountability for compliance rests with the Educational Bodies, not PowerSchool.

Reasonableness of the security measures

[46] Our assessment of the events associated with this Incident against the security measures set out in the agreements demonstrates flaws in PowerSchool's security measures. Recall that the cause of the Incident was reported by PowerSchool to be a cyberattack involving the use of stolen administrative level credentials (user ID and password) to access PowerSource, which enabled the threat actor to access the Personal Information of students, staff and parents/guardians stored in the SISs using the same set of stolen credentials.

PowerSource features

[47] To better understand the role of the PowerSource support application in the cybersecurity attack that led to the Incident, it is important to understand the relevant features of PowerSource and its role in PowerSchool's maintenance support operation.

[48] According to PowerSchool, PowerSource is a support application used by both PowerSchool and its clients for support maintenance services. The Educational Bodies used the PowerSource support portal to request maintenance support. PowerSchool uses the PowerSource application to remotely connect to the instances of SIS to perform support maintenance operations.

[49] In response to our question about how the PowerSource account was compromised and how support staff had access to PowerSchool systems from outside its network at the time of the Incident, PowerSchool's response was that some of its employees had role-based administrative level access to PowerSource, which allowed the employees to access SIS instances for maintenance and support activities. It added "[f]or the subset of customers who had enabled

remote support permissions, an employee with proper permissions could gain access to those customers' SIS database instances". This clarifies that the PowerSource application interfaces with the SIS and allows remote access to the SIS. It also clarifies that some of PowerSchool's employees who had access to PowerSource also had administrative level privileges, which gave them administrative level access to the SIS to perform support maintenance functions.

[50] The fact that PowerSource interfaces with the SIS and allows remote access to the SIS by employees with administrative level privileges makes PowerSource a critical resource. In addition, because PowerSource is a cloud-based (Software as Service) application that is accessible across the internet, it presents an attack surface to the SIS. This was also the case at the time of the Incident.

Summary of security measures set out in agreements

[51] In the agreements that PowerSchool entered into with the Educational Bodies, PowerSchool agreed to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk"[18] and to "safeguard and keep confidential personal or sensitive information obtained from the User(s), including, but not limited to personally identifying information"[19].

[52] It also agreed to "abide by and maintain adequate security measures, consistent with industry standards for digital storage of Customer Data, to protect Customer Data for unauthorized disclosure or acquisition by an unauthorized person"[20]. It then described in further detail some of these measures, as set out below (summarized by me), noting explicitly that the list provided is non-exhaustive:

- that it will secure usernames and passwords at a level meeting or exceeding the applicable standards;
- that it will maintain security protocols that meet industry standards including that data may only be viewed or accessed by parties legally allowed to do so and that it will maintain all data in a secure environment;
- that it will provide security training, periodically, to its employees who have access to the system;
- that it will employ industry standard measures to protect data from unauthorized access, which will include server authentication and that it will host the data using industry standard security controls that are updated according to industry standards;
- that it will provide the name and contact information of its security coordinator regarding customer data;

[18] 2024 DPAs.

[19] 2021 DPSs.

[20] 2024 and 2022 DPAs.

- that it will manage vendor sub-processors to ensure they abide by the agreement;
- that it will follow its security policies and protect it against such risks as unauthorized access, collection, use or disclosure or loss and that the security arrangements will include reasonable physical, administrative, and technical safeguards; and
- that it will have its security compliance assessed by third party auditors and will provide to customers on certain terms its ISO27001:2022 certification and SOC II Reports.

[53] In its data security and privacy plan, it further agreed to review its data security and global privacy statement and practices to ensure they are in conformance with applicable laws. In this same plan, it set out how it meets the requirements of ISO 27001:2022 or the NIST Cybersecurity Framework to protect the security, confidentiality and integrity of the data it receives under the agreements and set out a number of more granular measures to achieve this requisite security level. Below are those relevant to this investigation.

- Data leak protection is implemented
- Data destruction is performed according to the agreement
- A plan for vulnerability management is developed and implemented
- Log/audit records are maintained according to policy
- Credentials are issued, verified, managed, audited, and revoked as applicable
- Remote access conforms to ISO 27001:2022 standard
- Any breaches will be managed, and prompt notification will be provided[21]

[54] It also addressed how it would manage breaches and the termination and destruction of records. Included in the paragraph about breaches, it states that it will "notify the customer without delay, and within 72 hours where access is by a third party". For termination and destruction, it provided that it will return or delete any personal information of the customer on written request, that it may facilitate transfer instead, and that it will not regain the information beyond the necessary period for decision and notify the customer when all the information has been returned/disposed/deleted.

[55] The standards referenced in the agreements, ISO 27001:2022 and the NIST (National Institute of Standards and Technology) Cybersecurity Framework (NIST CF) are internationally-recognized security frameworks that guide industry best practices for information security. Both, generally, set out a framework consisting of governance together with recommended security measures consisting of administrative, technical and physical security controls that are intended to protect system infrastructure and data processed or otherwise stored therein.

[56] Below we assess the security measures relevant to what occurred in the Incident to determine if PowerSchool's security measures implemented at the time of the Incident were as described in the agreements.

[21] While there were slight differences between the versions of the agreements, the representations regarding security measures were substantially the same in both.

Remote support permissions

[57] As indicated, the agreements specify that PowerSchool's security standards are aligned with those set out in ISO 27001:2022 and NIST CF.

[58] ISO 27001:2022 establishes guidelines for cybersecurity and privacy protection for information security management systems. This guideline sets out a security framework for an organization consisting of understanding the organizational landscape, leadership including policy and roles and responsibilities, planning to address risks through risk assessment and treatment, and support for compliance including documenting controls and communication of them, operationalizing of the framework, and evaluation and improvement. Specifically, the document is designed to "provide requirements for establishing, implementing, maintaining and continually improving an information security management system"[22] for an organization.

[59] In terms of security risk treatment, the guidelines specify that an organization shall select appropriate risk options taking account of the risk assessment results, noting that it must determine all controls that are necessary to implement the information security risk treatment option chosen.[23] The controls herein referenced are contained in an appendix to the guidelines. Those relevant to remote access are listed below.

- *Control 5.34 Privacy and protection of personal identifiable information (PII)* requires an organization to identify and meet the requirements regarding the preservation of privacy and protection of PII (personally identifying information) according to applicable laws and regulations and contractual requirements.
- *Control 6.7 Remote working* requires the implementation of security measures when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.
- *Control 8.2 Privileged access rights* requires an organization to restrict and manage the allocation and use of privileged access rights.
- *Control 8.3 Information access restriction* requires an organization to restrict access to information or other associated assets in accordance with the established topic-specific policy on access control.
- *Control 8.5 Secure authentication* requires an organization to implement secure authentication technologies and procedures based on information access restrictions and the topic-specific policy on access control.
- *Control 8.8 Management of technical vulnerabilities* requires an organization to obtain information about its technical vulnerabilities of information systems and exposure to such vulnerabilities shall be evaluated and measures taken.

[22] At p. v.

[23] At p. 4.

- *Control 8.9 Configuration management* requires an organization to establish, document, implement and review configurations, including for security, of hardware, software, services and networks.

[60] The NIST Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD)[24] Security (NIST Remote Access Guide) establishes guidelines for security associated with, inter alia, remote access. It states the following (as summarized by me) about what is necessary to mitigate the risks associated with permitting remote access in recognition that "remote access technologies often need additional protection because their nature generally places them at higher exposure to external threats"[25].

- A remote access policy should define the forms of remote access an organization permits, and the type of access required for its staff and that the decisions made should be risk-based.

- Considerations in developing this policy include:
  - sensitivity of the data and compliance with mandates and other policies;
  - whether to prohibit remote access to sensitive personal information; and
  - the risks associated with providing a way for external actors to gain access to internal resources.

- Situations involving high risk require additional security requirements such as the use of multi-factor authentication.

- Threat modeling should occur to design a remote access solution to incorporate controls needed to meet the security requirements.

- Remote access policies and controls should be developed on the assumption that client devices will be acquired by malicious parties who will either attempt to recover sensitive data from devices or leverage the devices to gain access to the enterprise network.

- Threats can be mitigated against an attacker gaining remote access and impersonating a user by using strong authentication, preferably multi factor, for enterprise access.

- Access to internal resources accessible through remote access should be hardened appropriately against external threats and any access limited to the minimum necessary through firewalling or other access control mechanisms.

- Careful planning must occur for remote access client software security before selecting and deploying a remote access solution because if not properly secured, it can be misused by attackers to access a client's internal resources.

[24] Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (nist.gov).

[25] *Ibid,* at p.2.

- A remote access client should be "thick" such that the client has nearly complete control over the remote access environment.

[61] We asked PowerSchool about whether its support staff had remote access to SIS. The response provided is below.

> *At the time of the breach, some employees had role-based administrative level access to PowerSource. This access allowed employees to log into SIS instances for maintenance and support activities. For the subset of customers* ***who had enabled remote support permissions****, an employee with proper permissions could gain access to those customers' SIS database instances.* [Bolding mine]

[62] This response suggests that access to the Educational Bodies' instances of the SIS could occur remotely through the use of the PowerSource application if the Educational Bodies enabled remote support permission in their instances of SIS.

[63] PowerSchool stated further in regard to this access "[f]or the subset of customers who had enabled remote support permissions, an employee with proper permissions could gain access to those customers' SIS database instances."

[64] The ability to remotely access these SIS instances meant that without proper controls in place regarding this access, there could be persistent remote access connections between PowerSource and the Educational Bodies' instances of the SIS.

[65] To determine whether this was the case, we contacted five Educational Bodies who hosted their instances of SIS on-premises to better understand how they managed remote access to the SIS via PowerSource for maintenance support operations. We specifically asked these Educational Bodies to describe how the PowerSource application established connectivity with their instances of SIS prior to and up to the time of the cyberattack in December 2024, and to clarify if such connectivity was persistent or done upon request (on-demand)[26]. We also asked them to clarify if such connectivity was on-demand and if they were receiving maintenance support services from PowerSchool during the time of the Incident between December 19, 2024 and December 28, 2024.

[66] Three of the Educational Bodies advised us that PowerSchool had two methods to provide remote support operations. For the first method, PowerSchool would initiate a remote connection that would allow the Educational Bodies to download and run a remote connection client software. Through that software, the Educational Bodies would authorize PowerSchool staff to access their instances of SIS for support purposes. After the support was completed, the connection was terminated. The second method was via the PowerSource application.

[67] Regarding use of PowerSource to remotely access instances of SIS which were on-premises, four Educational Bodies stated the following:

[26] A persistent connection is one where the established network connectivity remains active at all times, whereas an on-demand connection occurs upon request and once the specific support activity is completed, the connectivity is terminated.

- *Enable Remote Support feature in PowerSchool prior to the Dec 2024 breach, this was an unlimited On/Off setting with no expiry. It was a persistent connection type. At the time of the breach, it was set to On. Subsequent to the breach, they made this time limited. It is not possible as far as I am aware to tell when this was enabled prior to the breach.*

- *Apparently,* [the enabled remote support feature in PowerSource] *was the default setting by PowerSchool previously. After the incident, they instructed everyone to disable the remote support option.*

- *Unbeknown to us, there was a secondary method enabled (PowerSource Support application) that can be used on demand through the support portal by PowerSchool support engineers (without so much as multi-factor authentication). This did not require any intervention or action on our part to establish access. We were made aware of this secondary method, as well as how we could disable it after the breach.* ***The fact that we are self hosted, in the cloud made no difference****. To my understanding this is the exact same method that was used to access PowerSchool instances across North America regardless of whether they are hosted, self hosted, in the cloud or on premises. PowerSchool later released an update that removed this feature altogether. None of our staff were aware of, or have previously used the PowerSource Support application when obtaining support.* [Bolding mine]

- *Before the December 2024 breach,* [we] *had an open portal allowing PS Support access when it was needed and stayed open (persistent connection). The ability to connect at any time was active, but connections were terminated when the ticket was resolved.*

[68] One of the Educational Bodies hosted its own instance of SIS in its own cloud. Its instance of SIS was compromised using PowerSource because the remote support feature for its SIS was enabled by default.

[69] The fact that the threat actor made their way into many instances of SIS in PowerSchool's cloud suggests that all these instances had their respective remote support feature for their instances of SIS enabled by default.

[70] We asked PowerSchool about how it managed remote access at the time of the breach and how the remote access control conformed to the ISO 27001:2022 standard at the time of the breach. PowerSchool responded as follows.

> *PowerSchool's Access Control Policy provides for secure channel controls for remote access to PowerSchool's network and systems to minimize the potential exposure from unauthorized use of PowerSchool's resources. PowerSchool's last ISO 27001:2022 Recertification Audit Report was prepared by A-LIGN Assurance in March 2024 and included, among other PowerSchool applications, PowerSource in the scope of the assessment and certification.*

[71] The above evidence demonstrates that prior to and up to the date of the Incident, the Educational Bodies had little or no ability to control remote access to their instances of SIS via PowerSource. According to the submissions of these Educational Bodies, they were unaware that the "remote support feature" was enabled by default in their instances of SIS.

[72] This persistent access to the Educational Bodies' instances of SIS enabled the threat actor to exploit the enabled remote access feature using PowerSource to trigger a maintenance operation to access various instances of the SIS and exfiltrate information, including the Personal Information. According to the Crowdstrike report, "the threat actor performed Maintenance Remote Support operations in PowerSource, which enabled the threat actor to access the individual customer organizations' SIS instances."

[73] As indicated, ISO 27001:2022 requires an organization to: implement security measures when information may be accessed outside an organization; restrict and manage access rights; restrict access to information; implement secure authentication technologies; identify and address technical vulnerabilities; and to configure software so that it is secure. Had PowerSchool undertaken these activities for the remote support feature, it likely would have identified that the remote support feature of the instances of SIS was enabled by default and disabled it. Either PowerSchool knew of this risk and did not address it, or it was not aware of this security risk. Either way, the fact that these instances of SIS had the remote support feature enabled by default created a significant security risk for the Educational Bodies that was ultimately exploited by the threat actor and resulted in the exfiltration of the Personal Information.

[74] Turning now to NIST CF, this standard requires an organization to: make decisions about remote access based on risk and to consider the sensitivity of information accessible remotely in making decisions; to threat model such that the remote access solution is designed to ensure security; to assume, in determining an adequate level of controls, that a threat actor will attempt to gain access to client information; to harden remote access to mitigate against external threats; and to structure remote access in such away to ensure its clients are thick, i.e., have nearly complete control over the remote access environment. For the reasons noted above, it is clear that this standard was not met in regard to the default enabled remote support feature of the Educational Bodies' instances of SIS.

[75] In my Preliminary Investigation Report, I concluded that the enabled remote access by default through PowerSource to access the Educational Bodies' instances of SIS for maintenance failed to meet industry standards. I further concluded that this failure falls below what constitutes "reasonable security arrangements" in section 38 of the FOIP Act.

[76] In its representations to the Preliminary Report, PowerSchool challenged my findings and conclusion on the basis that, according to PowerSchool, the remote access feature to access the Educational Bodies' instances of the SIS was not enabled by default at the time of the Incident, but had to have been enabled by the Educational Bodies. In this regard it stated:

> **[Several] [p]*aragraphs***…*are premised on an assertion that maintenance access was "enabled by default." This is incorrect. At the time of the Incident, maintenance access through PowerSource was set to "on" by default only for the first 30 days following installation of a new SIS instance. After 30 days, the default switched to "off" and customers thereafter requiring maintenance access to their SIS through PowerSchool would need to change the setting to "on." Only the customer could control this setting, and customers were advised to keep maintenance access "off" unless support was necessary.*
> [Bolding in original]

> *PowerSchool requests that the IPC revise* [several] *paragraphs and related findings in* [another] *paragraph to reflect the true settings on PowerSource maintenance access at the time of the Incident, as described above.*

[77] In its representations about this security measure, it added:

> *Access Path and Scope. The compromised credentials provided access to PowerSource's maintenance access tool. This tool enabled access to customer SIS instances only where a customer's SIS administrator had set maintenance access to "on." This setting was not globally "on" nor universally applicable. It did not confer broad administrative control. PowerSchool respectfully requests that the IPC add additional details to reflect that the threat actor gained access only to customer SIS instances where the customer had maintenance access set to 'on' in their settings.*

[78] Also, in its representations, in the section "CORRECTIVE ACTIONS TAKEN BY POWERSCHOOL SINCE THE INVESTIGATION" it identifies as a corrective action "[r]emoval of the "always on" maintenance access option for SIS customers, and limitation of maintenance access duration to no more than 30 days, with the duration set by the customer's SIS administrator". I note that the phrase "always on" means that this feature was persistently on. Also, the "always on" corroborates the statements of the Educational Bodies regarding this feature being persistently active within their instances of SIS prior to and up to the Incident.

[79] The representations made by PowerSchool regarding access to customers' instances of SIS for maintenance does not align with the Educational Bodies' submissions about what occurred in terms of the threat actor's ability to access their respective SIS instances and is in certain aspects conflicting.

[80] It is clear from the facts surrounding the Incident that the threat actor was able to access these Educational Bodies' instances of the SIS, meaning that the maintenance access to these instances had to have been 'on' given that PowerSchool reported this was the only way the threat actor compromised the instances of the SIS. Given that the remote access feature was 'on' for all of these Educational Bodies appears to indicate that this was a default configuration that was always on.

[81] Recall that the four Educational Bodies with on-premises instances of their SIS stated the following about the remote maintenance feature on their respective SIS instances.

- *Enable Remote Support feature in PowerSchool prior to the Dec 2024 breach, this was an unlimited On/Off setting with no expiry. It was a persistent connection type. At the time of the breach, it was set to On.* ***Subsequent to the breach, they made this time limited. It is not possible as far as I am aware to tell when this was enabled prior to the breach****.*

- ***Apparently,*** **[the enabled remote support feature in PowerSource]** ***was the default setting by PowerSchool previously****.* ***After the incident, they instructed everyone to disable the remote support option.***

- ***Unbeknown to us, there was a secondary method enabled (PowerSource Support application) that can be used on demand through the support portal by PowerSchool support engineers***

> *(without so much as multi-factor authentication)****. This did not require any intervention or action on our part to establish access. We were made aware of this secondary method, as well as how we could disable it after the breach****. The fact that we are self hosted, in the cloud made no difference. To my understanding this is the exact same method that was used to access PowerSchool instances across North America regardless of whether they are hosted, self hosted, in the cloud or on premises. PowerSchool later released an update that removed this feature altogether.* ***None of our staff were aware of, or have previously used the PowerSource Support application when obtaining support****.*
>
> - ***Before the December 2024 breach,*** **[we]** ***had an open portal allowing PS Support access when it was needed and stayed open (persistent connection)****. The ability to connect at any time was active, but connections were terminated when the ticket was resolved.*
>
> [Bolding mine]

[82] As can be seen, two of the Educational Bodies were unaware of the feature and only learned about it as a result of the breach. All indicated that changes were made to the feature after the breach, which appears to align with PowerSchool's submissions regarding post Incident corrective actions made to the feature.

[83] The evidence of these Educational Bodies and that of PowerSchool make it clear that the remote access feature was 'on' for all of the Educational Bodies involved in the Incident and all the educational bodies affected by the Incident across North America as default configuration of the various instances of the SIS that was always on. The troubling aspect of the "always on" remote feature is that, as reported by the Educational Bodies, it was not being used for the remote support it was designed for. As explained by the Educational Bodies, remote support from PowerSchool was via a remote access client authorized by the client. Having this feature always on was an exploitable vulnerability that was exploited by the threat actor to compromise these SIS instances.

[84] The very scale of the attack alone, involving educational institutions across Canada and the US and impacting more than 60 million individuals, puts into question the credibility of PowerSchool's evidence that the remote access feature for all these instances of SIS was not enabled by default.[27] At the very least, the evidence demonstrates that there was a lack of technical controls implemented by PowerSchool to mitigate the risks of remote access to these instances of SIS.

Conclusion about remote support permissions

[85] Even if the remote access was not enabled by default, which is highly unlikely given the evidence, the evidence shows that PowerSchool failed to implement appropriate controls in alignment with the ISO27001:2022, NIST CF and NIST Remote Access standards to securely manage remote access to the SIS instances. Therefore, I conclude that PowerSchool's failure to identify and address the

[27] As reported by multiple news sources, the breach impacted at least 62.4 million students and 9.5 million teachers globally and affected multiple countries, including Canada and the US. In Canada alone, at least 80 Canadian school boards were affected.

risks posed by enabling persistent remote access to these SIS instances falls below what constitutes "reasonable security arrangement" in section 38 of the FOIP Act.

[86] I will add here that having the remote access feature turned on persistently for 30 days still falls below the security standards referenced above because as a security measure, systems need to be hardened by disabling features that are not required and only turning on those features when they are required for support functions. Having the remote access feature always on appears to indicate that these instances of SIS were not hardened when they were implemented or that they were poorly hardened, making them vulnerable to attacks. In my view, leaving unnecessary remote access to an application persistently open falls below industry standards.

Privileged accounts

[87] Generally, privileged account holders have elevated privileges that enable them to have broader access privileges to systems and information therein to perform system administrative functions, such as maintenance support operations, which standard users do not have and cannot do. Such privileges were associated with the compromised PowerSource account that the PowerSchool contractor had to provide maintenance support operations for the instances of the SIS.

[88] In terms of privileged accounts, ISO 27001:2022 establishes the following control in relation to this type of account.

- Control 8.2 Privileged access rights requires organizations to restrict and manage the allocation and use of privileged access rights.

[89] In addition to the security controls mentioned above as contained in the NIST CF, these guidelines state the following about the use and management of privileged accounts.

- Security measures that are particularly important for remote work include that remote workers "should use their limited privilege accounts for regular work and use a separate administrator account only for tasks that require administrative-level access, such as software updates [because] this reduces the likelihood of an attacker gaining administrator level access to the PC"[28].

[90] PowerSchool's access control policy states, in part,

> *System administrator accounts will not be granted direct remote access to any PowerSchool network or application. System administrators must authenticate to the network using their standard account credentials and then, if performing any system administrator job function, authenticate using their unique privileged level account credentials.*

[91] According to this policy, a system administrator account holder would be prevented from using their privileged account credentials to log into PowerSchool's network and could only access this network using their standard network access credentials. Once within the network, the privileged account holder could then log into an application, such as PowerSource, using their privileged

[28] At p.33.

account credentials to perform maintenance support operations, amongst other things, after being successfully authenticated. Generally, system administrator accounts have the highest level of privileges.

[92] Having such a policy is necessary to reduce the risks that would flow from the compromise of system administrator account credentials which enables the account holder to perform a wide range of functions including modification of system configuration and data, data exfiltration, and creation of new accounts in the system. PowerSchool's policy concerning system administrator accounts as described appears to be consistent with the NIST standard for privileged account holders.

[93] Below is a description of what occurred in relation to the use of a privileged account by the threat actor.

- The attacker used PowerSource to infiltrate PowerSchool's network. PowerSource is SaaS (Software as a Service) and hence a web application with a user interface. Behind that interface is the application server that hosts the PowerSource application within PowerSchool's network. Since PowerSource is a SaaS, it is accessible via the internet from anywhere because it is a public-facing application. What the threat actor did was use the stolen set of credentials of the contracted support staff (user ID and password) to get in. Once in PowerSource, the attacker enabled the remote support service, which led the attacker to have visibility into instances of SIS that also (as indicated above) had remote support service enabled. This is because PowerSource interfaces with SIS making it possible to identify which instance of SIS interfaces with PowerSource. When the attacker used the enabled remote support service to initiate connection with the instances of SIS, the attacker was required to authenticate to access those instances of SIS. Using the same stolen set of stolen credentials, the attacker authenticated and gained access to those instances of SIS because the contracted support staff had the same set of credentials for this access.

[94] We asked PowerSchool about how system administrator accounts were created and managed at the time of the Incident. PowerSchool responded "PowerSchool policy states that administrative accounts will not be granted direct remote access to PowerSchool networks or applications", which merely restates the access control policy without any explanation as to how, in this case, system administrator credentials were used to access both PowerSource and the SIS instances.

[95] We also asked PowerSchool about how its system administrators accessed PowerSchool's systems remotely. It responded as follows, again with no explanation about how the same credentials were used to access PowerSchool's network and PowerSource.

> *At the time of the breach, some employees had role-based administrative level access to PowerSource. This access allowed employees to log into SIS instances for maintenance and support activities. For the subset of customers who had enabled remote support permissions, an employee with proper permissions could gain access to those customers' SIS database instances.*

[96] In my Preliminary Investigation Report, I concluded that PowerSchool had violated its access control policy on the incorrect assumption that the stolen account credentials were 'system

administrator'. PowerSchool's representations concerning this assumption and my conclusion are as follows:

> **[Several] [p]*aragraphs…*** *assume that the compromised credentials conferred administrative access or were used to access "SIS administrative accounts." That is inaccurate. The relevant account had maintenance access through PowerSource as part of a Support Engineer role. Maintenance access is limited, task-specific access used to perform support functions and does not confer broad, persistent control over systems or customer data; by contrast, "administrative privileges" refers to elevated, discretionary rights (e.g., user/account management and unrestricted configuration or data access). This distinction is material to assessing PowerSchool's safeguards at the time.*
>
> *Further, the compromised PowerSource credentials enabled the use of the maintenance access tool to access certain customer SIS instances. Once authenticated, the Support Engineer could access, through PowerSource, SIS instances of customers with maintenance access enabled by inputting the URLs of SIS instances, which were generated using information available online. The credentials did not confer SIS administrative account access or administrative privileges across PowerSchool products. The PowerSource maintenance access tool did not provide access to other PowerSchool applications.*
>
> *PowerSchool requests revisions to* [several] *paragraphs, and related findings in* [another] *paragraph to substitute "maintenance access" for any reference to "administrative" level privileges and remove references to SIS administrative account access.*
> [Bolding in original]

[97] Based on these representations, I have addressed the references regarding the use of 'system administrator accounts' in relation to the account credentials used by the threat actor in the Incident as applicable herein. I will now assess this new evidence against the standards described above for privileged accounts.

[98] While the account credentials used by the threat actor were not for 'system administrator accounts' in the sense that they gave the user broad system-level privileges, the account credentials were privileged, nonetheless. This is because, as represented by PowerSchool, these credentials gave the account holder privileged administrative level access to SIS instances to perform maintenance support services in the SIS. This type of account is a subset of "SIS administrative accounts" (noted above), with privileges based on specific roles associated with the account.

[99] Having again reviewed PowerSchool's Access Control Policy against this kind of privileged level access, the policy does not mention this type of administrative level privilege. As indicated, it only references "system administrator privileges" and specifies the rules concerning those privileges, but is silent on other administrative privileges, such as those used for maintenance support. Given this, the policy is deficient and does not align with the standards as described above for privileged account holders. This gap in policy is likely the reason the account holder whose credentials were used by the threat actor in the Incident had the same credentials for logging into PowerSource and for authenticating to gain access to the SIS instances to perform maintenance.

Conclusion about privileged accounts

[100] Based on the foregoing evidence, my new conclusion is that PowerSchool's access control policy is deficient for the reasons indicated and does not meet the industry standards, as described above, for managing remote access by its privileged account holders. As a result of this and the fact that this gap is the likely cause of the threat actor's ability to gain access to the Educational Bodies' instances of SIS and to exfiltrate the Personal Information, I conclude that PowerSchool's security control concerning privileged account management falls below what constitutes "reasonable security arrangements" in section 38 of the FOIP Act.

Multi-factor authentication

[101] I am able to infer from the evidence before me about how the Incident occurred, i.e., the threat actor was able to access the SIS via PowerSource using a single set of authentication credentials, that there was no multi-factor authentication used for this access because had there been, the threat actor would not have been able to compromise PowerSource as reported.

[102] In terms of multi-factor authentication, ISO 27001:2022 has the following control.

- *Control 8.5 Secure authentication* requires an organization to implement secure authentication technologies and procedures based on information access restrictions and the topic-specific policy on access control.

[103] The NIST standard highlights (in relation to the risks associated with remote access) that if an organization has higher security needs, it should consider using authentication that does not rely solely on passwords, such as multi-factor authentication[29].

[104] We asked PowerSchool about the use of single-factor authentication for PowerSource instead of multi-factor authentication (MFA). PowerSchool's response was vague. It said "[a]ccess controls, including two-factor authentication controls varied across PowerSchool products and platforms".

[105] PowerSource and the SIS are cloud-based solutions, although some customers, as is the case with some of the Educational Bodies, host their SIS on premises. Cloud-based solutions are accessible via the internet. Using single-factor authentication for cloud-based solutions make them vulnerable to cyberattacks. Those customers, including, as indicated above, some of the Educational Bodies, which hosted their instances of SIS on premises with remote support permissions enabled in PowerSource, were also vulnerable to cyberattacks. The information accessible in the instances of SIS is highly sensitive, as indicated, and required PowerSchool to have advanced security measures in place that is proportionate to the sensitivity of the information, in order to protect the information. The industry standards, as identified above, require that this risk be mitigated through the use of MFA to access PowerSource and the instances of SIS. Consequently, the failure to implement this security safeguard by PowerSchool falls below industry standards for this environment.

[29] At p. 26, 41 and 42.

[106] According to the Crowdstrike forensics report, following the incident, PowerSchool implemented new security controls to secure the impacted environment. One of them was “requiring that access to the PowerSource environment be via company’s VPN, which requires single sign-on (SSO) and multi-factor authentication (MFA)”.[30]

Conclusion about use of multi-factor authentication

[107] Based on the foregoing, I conclude that PowerSchool failed to meet the industry standard of using MFA for access to PowerSource and cloud-based instances of SIS. Failure to meet these standards falls below the standard of “reasonable security arrangements” in section 38 of the FOIP Act.

Password policy and the use of secure credentials

[108] The fact that the threat actor used compromised (stolen) credentials of a PowerSchool contractor with administrative level privileges to compromise the SIS demonstrates that PowerSchool may have failed to reasonably secure these authentication credentials.

[109] We asked PowerSchool to provide information about its password policy that was implemented in PowerSchool systems at the time of the breach, including the password policy implemented in PowerSource and the SIS. We asked PowerSchool to provide information about password length, complexity, composition, and expiration rules, including the number of iterations before an old password is allowed to be reused. PowerSchool responded to these questions as follows:

> *PowerSchool’s password policy follows the latest NIST guidelines on password, strength, complexity, and rotation.*

[110] According to NIST Special Publication (SP) 800-63B,[31], section 3.1.1.2 Password Verifiers requires that passwords that are used as a single-factor authentication mechanism be a minimum of 15 characters in length and when used as part of multi-factor authentication processes be a minimum of eight characters in length.

[111] On review of PowerSchool’s password policy, we found it deficient because it contains no requirements for password complexity, composition, expiration and rules regarding how many iterations are allowed before an old password can be re-used. The password policy states that “passwords must be a minimum of eight characters”. PowerSchool’s minimum password length of eight characters is below the NIST standard when used as a single-factor authentication, which was the case here. The standard applicable for a password length for a password used without multi-factor authentication is a minimum of 15 characters.

[112] We asked PowerSchool about the security controls it had in place at the time of the Incident to secure usernames and passwords, including the controls to protect passwords in password databases and how they meet or exceed industry standards as claimed by PowerSchool. PowerSchool responded with a general response setting out its controls.

> *PowerSchool has a strict password policy, which requires employees to complete the password governance policy annually. PowerSchool expects that all employees comply with various security*

[30] At p.3.

[31] NIST Special Publication 800-63B.

> *measures, such as strong passwords in compliance with PowerSchool's encryption policies, maintaining passwords of complexity and length, and securing passwords through appropriate methods and processes.*

[113] We also asked PowerSchool about the steps it took to ensure that selected passwords by its employees are not already compromised passwords, and other steps taken to enhance password security. In response, PowerSchool provided the following information without any explanation about how the credentials used in the cyberattack may have been compromised.

> *Users are restricted from storing or transmitting passwords in clear text or without use of authorized encryption, sharing passwords with any other person, reusing passwords between systems, or locally storing or "remembering" passwords within an unapproved system or application.*

[114] In responding to these questions, PowerSchool did nothing more than state its policies concerning password security and management and provided no evidence about whether it met this policy as it relates to the credentials used by the threat actor in the Incident or what steps it took, if any, to determine how these credentials were compromised.

[115] Educational Bodies, as public bodies under the FOIP Act, have, in an investigation about the privacy provisions therein, an evidential burden to show that they met their respective duties in regard to these provisions, including meeting their respective duties under section 38 to protect the personal information that was involved in the incident.[32] As an employee of these respective public bodies, PowerSchool must provide sufficient evidence to meet this burden, which it has not done.

[116] In my Preliminary Investigation Report, I concluded that, based on the foregoing evidence, PowerSchool failed to follow industry standards in creating its password policy and that this policy falls below the standard of "reasonable security arrangements" in section 38 of the FOIP Act. I also concluded that the Educational Bodies had failed to meet their evidential burden to establish that PowerSchool took any steps to determine how the credentials were compromised following the cyberattack, and found on that it did not take any steps.

[117] In its representations to the Preliminary Report, PowerSchool took issue with my findings and conclusions regarding its password policy, stating as follows:

> ***[Several] [p]aragraphs*** *of the Draft Report characterize PowerSchool's password policies as below reasonable standards. The compromised password was complex ("nfk4coxvpo"). PowerSchool's Information Security Management System (ISMS) Governance Policy and Access Management Policy impose strong password complexity and reuse requirements, including prohibiting reuse of the last five passwords. The presence of a complex password indicates the Incident did not result from lax password standards.*
>
> *PowerSchool requests revisions to* [several] *paragraphs and related findings in* [another] *paragraph to recognize that PowerSchool had developed, implemented, and enforced strong password policies.*

[118] These representations have not convinced me to change my findings or my conclusion concerning PowerSchool's password policy for the following reasons:

[32] See *University of Alberta v. Alberta (Information and Privacy Commissioner), 2009* ABQB 112 (CanLII), at para 108.

- The password provided was not 15 characters as required by the standards when used without multi-factor authentication. The password used was only 10 characters long.

- It was not a strong password let alone a complex password, having only lowercase letters and one number. There are no uppercase letters and special characters. This is below what is considered a complex password according to current standards. This password can easily be compromised using publicly-available password cracking tools.

- For the reasons indicated herein, the policy itself is deficient as measured against the standards referenced above.

[119] Furthermore, in its representations, PowerSchool did not provide any evidence about any steps it took to determine how the credentials were compromised after the cyberattack. As such my prior conclusion on this matter stands.

Conclusion about password policy and use of secure credentials

[120] Given the evidence that PowerSchool failed to follow industry standards in creating and enforcing a strong password policy, I conclude that this policy falls below the standard of "reasonable security arrangements" in section 38 of the FOIP Act. I also conclude that the Educational Bodies have failed to meet their evidential burden to establish that PowerSchool, an employee of these bodies, took any steps to determine how the credentials were compromised following the cyberattack, and, therefore, I find that it did not take any steps.

Network segregation

[121] From the evidence provided, it was unclear if PowerSchool had, at the time of the Incident, segregated PowerSource network environment from the SIS network environment. Network segregation partitions a network into zones of security, which provides an additional layer of security because systems and services in one network segment are screened or isolated from all other network segments. In the event of a compromise within a network segment, other network segments are not affected. Within this environment, when a system or user requires access to a service across a network segment, authentication and authorization is required from the network segment from which the services are requested. Without such authentication and authorization, such a request is denied.

[122] In terms of network segregation, ISO 27001:2022 sets out the following security controls.

- *Control 8.20 Network security* requires an organization to secure, manage and control networks and network devices to protect information in systems and applications.

- *Control 8.22 Segregation of network services* requires an organization to segregate in the organization's networks groups of information services, uses and information systems.

[123] In the NIST CF it states as follows.

- Organizations should carefully consider the security of any solutions that involve running a remote access server on the same host as other services and applications. Such solutions may offer benefits, such as equipment cost savings, but a compromise of any one of the services or applications could permit an attacker to compromise the entire remote access server. Placing the remote access server on a separate, dedicated host reduces the likelihood of a remote access server compromise and limits its potential impact. Using a separate host may also be advisable if the remote access server is likely to place other services and applications at significantly increased risk. An organization should also consider using multiple remote access solutions if its remote access users have vastly different security needs, such as one group accessing typical low-risk resources and another group accessing mission-critical confidential data.[33]

- Network integrity is protected, incorporating network segregation where appropriate, which involves segmenting a network (e.g., using subnetworks) to keep publicly accessible components off internal networks, and monitoring and controlling communication at key boundary points.[34]

[124] We asked PowerSchool about whether it had identified the risks of not segregating PowerSource and the SIS environment into separate security zones, PowerSchool responded as follows.

> *PowerSchool holds an International Organization for Standardization ("ISO") 27001 certification, as well as System and Organization Controls ("SOC") 2 Type 2 certifications for many of its core products. These certifications require multiple assessments of PowerSchool's core products, including the SIS, conducted by third-parties. The 2024 assessment on PowerSchool's Systems, including the SIS, 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." PowerSchool was not made aware of why specific risks were not previously identified during these assessments. PowerSchool is implementing additional safeguards to identify and prevent similar intrusions from occurring in the future.*

[125] When providing the Preliminary Investigation Report to PowerSchool for its representations, we asked it to address the lack of clarity about whether PowerSource was segregated from the SIS environment. It provided the following representations regarding the same.

> [Several] [p]*aragraphs…suggest inadequate network segregation premised on the notion of SIS administrative access from PowerSource. In fact, PowerSource and the SIS were hosted on separate platforms and networks— PowerSource is hosted on Amazon Web Services (AWS), and the SIS is hosted on Microsoft Azure. For this reason, PowerSchool requests that* [these] *paragraphs…and related findings in* [another] *paragraph be revised or removed.*

[126] The information provided helps to clarify whether PowerSource and the SIS were segregated. The evidence is that they are segregated on the basis that PowerSource is hosted in the AWS environment and the SIS is in the Microsoft Azure environment. For the following reasons, I am of the view that this degree of segregation warrants further review.

[127] The concept of network segregation from a security standpoint is not just to divide a network into segments, but to apply reasonable security controls that ensure each network segment is isolated to prevent threats from moving freely across the network. If a network segment or a resource within the network segment is compromised, a threat actor can be contained within the compromised network segment. There are situations where two or more networks are connected to form one flat network (network without segmentation). What occurred in the Incident is that the threat actor moved from the AWS environment to Microsoft Azure, suggesting that either the

[33] At p. 23.

[34] At p. 49.

two networks were simply connected together to form one flat network or that the segmentation controls failed to isolate the two networks to ensure the attack was contained within AWS.

Conclusion about network segregation

[128] Based on the foregoing evidence, I am not satisfied that PowerSchool had securely segmented the different environments that host PowerSource and the SIS. This is because the segmentation implemented by PowerSchool failed to prevent the threat actor from moving between the segmented environments suggesting additional controls are needed to prevent another breach from occurring. Given this, it is my conclusion that the segmentation utilized falls below the standard of "reasonable security arrangements" in section 38 of the FOIP Act.

Security risk assessments

[129] Both ISO 27001:2022 and the NIST CF include in the governance portions of these documents the need to conduct security assessments, particularly on remote access environments,[35] to measure performance of security controls and to use the findings to address any gaps or issues.

[130] PowerSchool provided copies of its SOC 2 Type 2 audit report completed by a third party for the period of July 1, 2023, to June 30, 2024, and a penetration test report completed by a different third party for the period of April 30 to June 25, 2024. Penetration tests are used to determine if security controls are functioning as expected and require identification and exploitation of security vulnerabilities in real time during the test.

[131] Having reviewed these documents, we asked PowerSchool about why these assessments did not detect the risk of using single-factor authentication to access PowerSource from the internet. PowerSchool responded as follows.

> *PowerSchool holds an International Organization for Standardization ("ISO") 27001 certification, as well as System and Organization Controls ("SOC") 2 Type 2 certifications for many of its core products. These certifications require multiple assessments of PowerSchool's core products, including the SIS, conducted by third-parties. The 2024 assessment on PowerSchool's Systems, including the SIS, 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." PowerSchool was not made aware of why specific risks were not previously identified during these assessments. PowerSchool is implementing additional safeguards to identify and prevent similar intrusions from occurring in the future.*[36]

[132] Here, PowerSchool confirmed that these assessments were conducted on its "core products". According to the SOC2 Type 2 report, the scope of the SOC2 Type 2 assessment included PowerSchool Cloud Solutions vis-à-vis enrollment, PowerSchool SIS, eSchoolPlus, Schoology, PM Assessment, Special Programs and Naviance Services System. Based on this list, PowerSource was out of scope for this assessment.

[133] The scope of the target systems for the penetration test included PowerSchool SIS Core-Admin, PowerSchool SIS Core-Teacher, PowerSchool SIS Core-Parent and Student, Data Exchange (DEX)

[35] ISO 27001:2022 6.1.2 and 8.2, and NIST Guideline at p.48.

[36] For clarity, PowerSchool provided this same response to multiple questions, which is why this response is duplicated.

Cloud, SIS iOS App, SIS Android App and One Roster API. This means that PowerSource was again out of scope for the penetration test.

[134] Because PowerSource was not in scope for these two assessments, the vulnerability associated with the use of single-factor authentication, the use of the same set of credentials by the support staff to access both PowerSource and the SIS, and the enabled remote support feature could not have been identified by these assessments.

[135] Recall that PowerSchool stated the following about remote access of its employees:

> *At the time of the breach, some employees had role-based administrative level access to PowerSource. This access allowed employees to log into SIS instances for maintenance and support activities. For the subset of customers who had enabled remote support permissions, an employee with proper permissions could gain access to those customers' SIS database instances.*

[136] This statement outlines the importance of PowerSource providing ongoing maintenance and support to the SIS. It also indicates that PowerSource integrates with the SIS, which stores the 'crown jewels', the Personal Information. Also, recall that system administrator support staff have administrative level access to PowerSource and the SIS. From a risk assessment standpoint, these facts clarify that PowerSource is an attack surface to the SIS and should have been considered in scope for the security assessments.

[137] In the agreement, PowerSchool represented that it has its security compliance assessed by third party auditors regarding its ISO27001:2022 certification and SOC II reports, which it did do as indicated by the documents provided to us for review. However, we found that PowerSource was out of scope for these assessments and the vulnerabilities that enabled the attack to occur were not assessed and, therefore, not addressed. It is up to an organization to identify the scope of such an assessment undertaken by a third party because the organization knows its information security infrastructure best and is in the best position, for a number of reasons, including cost, to determine the parts of its infrastructure that it wants assessed. The fact that PowerSource was not assessed meant that the vulnerabilities which were exploited by the threat actor and led to the Incident were not identified and addressed.

Conclusion about security risk assessment

[138] For the reasons indicated, this failure to assess PowerSource falls below what is required by section 38 of the FOIP Act to reasonably protect the Personal Information.

Breach reporting

[139] In the agreement, PowerSchool represented that it would notify a customer "without delay and within 72 hours where access is by a third party". As set out in the background section of this Investigation Report, the Educational Bodies received notification from PowerSchool about the Incident, which occurred on December 28, 2024, on January 7, 2025[37]. PowerSchool did not inform these bodies about why it had not notified them as required by the agreement. In any

[37] As determined by reviewing the breach reports received from the Educational Bodies.

event, in not doing so PowerSchool did not notify as agreed to in the agreement. Breach reporting in a timely manner is the key policy objective in breach notification requirements. Individuals who are at risk of harm from a breach, as was the case here, can only reasonably protect themselves from the harm if they receive timely notification. Failure to provide timely notification exacerbates these risks to the students, parents/guardians and teachers whose personal information was involved in the Incident and left the Educational Bodies in the difficult situation of having to explain to these affected individuals about the delay in notification.

[140] In my Preliminary Investigation Report, I concluded, based on the foregoing, that having enforceable breach management policies is an integral part of any information security program. However, at the time of the Incident, breach reporting and notification were not mandatory requirements in the FOIP Act, but were considered best practices. Given this, I concluded that the failure to notify the Educational Bodies as required by the agreement is a violation of the agreement but does not amount to non-compliance by the Educational Bodies in regard to their section 38 obligations.

[141] In its representations to the Preliminary Investigation Report, PowerSchool stated the following about why it did not report the breach until January 7, 2025 to the Educational Bodies.

> **[Several] [p]*aragraphs…***suggest PowerSchool failed to notify Educational Bodies within contractual timeframes. That conclusion conflates initial detection of a security event with confirmation of a reportable breach. A ransom note was received on December 28, 2024, triggering containment and forensic analysis. Targeted notifications began as early as January 7, 2025, following forensic confirmation of affected data and institutions. Where agreements tie notice to confirmation, a ten-day interval was reasonable to ensure accuracy and utility of the notice. In addition, not all customers experienced data exfiltration, necessitating validation before issuing notifications.*
>
> *PowerSchool requests that* [these] *paragraphs and related findings in* [another] *paragraph be revised or removed to reflect that PowerSchool provided prompt, accurate notifications upon confirmation of the Incident.*

[142] In a footnote following the first sentence above, which I omitted from the same, PowerSchool stated “PowerSchool also denies the allegations at [several] paragraphs of the Draft Report to the extent they suggest that PowerSchool in any way breached its contracts with Educational Bodies”.

[143] I accept that it takes time to assess whether a breach has occurred and that notification on January 7, 2025 about the incident, which was discovered on December 28, 2025, may be reasonable depending on the circumstances. However, as indicated above, the agreement specifies that PowerSchool would notify a customer “without delay and **within 72 hours where access is by a third party**” (bolding mine). The latter part of this sentence dictates what PowerSchool was to do on discovering it was the victim of a cyberattack (access by a third party) which then triggered its duty to notify the Educational Bodies within 72 hours. As such, my conclusion on this matter stands.

Conclusion about breach reporting

[144] I conclude that the failure to notify the Educational Bodies as required by the agreement is a violation of the agreement but does not amount to non-compliance by the Educational Bodies in regard to their section 38 obligations.

Monitoring of systems and network intrusions

[145] According to the Crowdstrike forensics report, during the investigation of the December 2024 Incident, PowerSource logs showed that an unknown actor successfully accessed the PowerSchool PowerSource portal using the compromised credentials. The report further states that 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.

[146] The report also states that at the time of the breach, PowerSchool's endpoints and servers were protected by CrowdStrike's Falcon Endpoint Detection and Response (EDR) software, which provides advanced security monitoring, threat detection, next-generation antivirus, and real-time endpoint detection and response (EDR) capabilities. The report adds that PowerSchool's systems are protected by CrowdStrike's Falcon Overwatch, a 24/7/365 threat hunting service.

[147] Both ISO 27001:2022 and NIST CF in the governance portions highlight the importance of monitoring systems for network intrusion. They also identify specific controls such as logging.

- ISO 27001:2022 *Control 8.15 Logging* requires an organization to have logs that record activities, exceptions, faults and other relevant events that are stored, protected and analysed.
- NIST has a specific guide dedicated to logging[38]. It sets out the following (as summarized by me).
  - Organizations should establish policies for log management including that clearly define mandatory requirements and suggested recommendations for log management activities, including log generation, transmission, storage, analysis, and disposal.[39]
  - Organizations should ensure logs are maintained for an appropriate period and analysed.[40]
  - Logs should be protected and stored.
  - Retention should be established based on applicable laws and policies, such as data retention, with the goal of balancing the organization's reduction of risk with the time and resources needed to perform log management functions.[41]

[38] Special Publication 800-92, Guide to Computer Security Log Management.
[39] At p.ES-1
[40] At p.21.
[41] At p. 41.

[148] The NIST logging publication has a chart[42] setting out examples of logging configuration settings. The relevant portions of the table are replicated below.

Category	Low impact systems	Moderate impact systems[43]	High impact systems
How long to retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months
How often log data needs to be analysed locally (through automated or manual means)	Every 3 to 24 hours	Every 15 to 60 minutes	At least every 5 minutes

[149] The meaning of low, medium or high impact is set out in FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.[44] Based on that table, the instances of SIS would likely fall into the moderate classification.

[150] Given that the compromises in August and September of 2024 were not detected by PowerSchool when they happened means that PowerSchool's monitoring controls failed to detect these attacks and issue appropriate alerts. This is an indication that PowerSchool's monitoring controls may not have been working as expected.

[151] In addition, there were no SIS logs to assist PowerSchool's forensic investigators in determining the impact of the August and September 2024 cyberattacks. This is because PowerSchool only stores its audit logs for 90 days and then they are deleted. As a result, PowerSchool could not know what activities took place during those two attacks.

[152] The lack of SIS logs associated with the August and September 2024 incidents leaves unanswered questions about whether any other personal information was compromised during those incidents.

Conclusion about monitoring and network intrusion

[153] Given that the SIS instances would be considered as moderate impact systems, the retention of PowerSchool's logs aligns with the recommended retention and, in fact, is at the higher end. I conclude, therefore, that its retention is sufficient and would meet the "reasonable security standard" in section 38 of the FOIP Act. That said, it is becoming more common for threat actors to go undetected for a number of reasons, which suggests the need to consider maintaining logs for a longer period. The fact that the intrusion was not detected by PowerSchool suggests that it needs to assess why this occurred and address the issue.

[42] At p. 44.

[43] An impact is 'moderate' if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals, and as to the latter could result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries. An impact is 'high' where said loss could be expected to have a severe or catastrophic adverse affect including to individuals that could result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries. At pp. 2 and 3 of linked source.

[44] At p. 10.

Decommissioning an SIS instance on termination of agreement

[154] One School Division that reported to us about the Incident informed us that they were surprised to learn that personal information of its students, staff and parents was involved in the breach. This is because this School Division thought this personal information had been deleted when the School Division stopped using its SIS instance in 2021. The School Division provided us with documentation setting out its communications with PowerSchool concerning its termination of the PowerSchool agreement in 2021.

- In a letter dated March 5, 2021, the School Division provided notice to PowerSchool that it was terminating its contract with PowerSchool citing its authority to do so under clauses 11 and 13.3 of the contract. The effective date of termination is stated therein to be August 31, 2021. The letter was delivered to PowerSchool by Purolator Courier.[45]

- On August 25, 2021, a PowerSchool Customer Services Manager emailed the Associate Superintendent of Business Services for the School Division and stated therein "…this email serves as confirmation that PowerSchool recognizes that the contract term date ends August 31, 2022[46] per the quote you will be signing and [the School Division] has no obligation to continue with PowerSchool past this date unless a new contract is negotiated". The Customer Services Manager added "I have also uploaded your email request to your account confirming that you do not plan to renew your subscriptions unless a new contract is signed".

- On July 8, 2022, a Technology Services Technician for the School Division emailed a PowerSchool representative, and stated "LRSD noticed that the SIS instance is still live at lrsd.powerschool.com. We have not used this service in over a year and would like the data purged from the PowerSchool infrastructure following your regular data retention policies [sic] however more importantly we require the live instance removed from the Internet ASAP", adding "[p]lease let us know when the instance is no longer live".

- On July 21, 2022, PowerSchool's Customer Success Manager II – Enterprise Canada replied "I have just received confirmation from internal teams that the Decommissioning is complete, the below instance is no longer available". Below this sentence is "lrsd.powerschool.com/admin".

[155] When the School Division received the notice from PowerSchool about the Incident, it engaged PowerSchool in the following communications.

- On January 7, 2024, the School Division's same Technology Services Technician emailed the Customer Success Manager II – Enterprise Canada for PowerSchool, copying the Senior Account Executive – Enterprise, Eastern Canada, and stated the following.

[45] As demonstrated by a pickup confirmation by Purolator which is attached to the letter.

[46] It is unclear if this date should have been August 31, 2021.

> *We received the alert today notifying compromised customers of the data breach. We are able to access our data still at this instance although we received confirmation in July 2022 that it was decommissioned. Can you tell us why the LRSD SiS data is still live even though we have cancelled our contract with Powerschool* [sic] *three plus years ago and what happened that the decommissioning you verified was reversed? We are booking into meetings tomorrow but would like a follow up as we see this issue beyond the initial cyber breach as it is against data that PowerSchool committed to purging and no longer retaining.*

- The Senior Account Executive – Enterprise, Eastern Canada forwarded the email internally to a number of individuals and cc'd the School Divisions' Technician, stating therein:

> *…Their main concern is that their PowerSchool SIS instance has been decommissioned in our system, but the logs that they are seeing shows activity in their instance from 11/26/25 onward.*
>
> *While they may not be on the list of affected customers, they believe that their data was accessed by PowerSchool [sic] and would like assistance on obtaining the appropriate instructions to pull log audits as well as a forensic report of the data that was accessed.*
>
> *Finally, they need to understand how to completely shut down their hosted instance of PowerSchool… They understand that we don't delete their data, but the hosted instance needs to be completely shut down…*

[156] The final email between the School Division and PowerSchool, dated January 10, 2025, confirms that the School Division's instance of the SIS was shut down by PowerSchool. Included in the email was a question posed by the School Division to PowerSchool asking whether the fact that it could not access its instance of the SIS is confirmation that its data is no longer live and accessible. The School Division indicated that it did not receive a response from PowerSchool to this question.

[157] This School Division provided us with a copy of its 2021 MSA and 2021 DPS with PowerSchool. It is unclear what specific clause in clause 11 was relied on by the School Division to terminate the agreement. I do not see a clause 13.3 in the agreement as referenced by the School Division in its letter. In any event, the response from PowerSchool confirms that the contract was to be terminated as of August 1, 2021[47].

[158] Clause 1.3 of the DPS clarifies that the customer controls all their data.

[159] Clause 2 addresses the return and disposition of data. It states:

> ***2.1.*** *Upon written request and in accordance with the applicable terms in* ***Sections 2.2 or 2.3,*** *below, PowerSchool will dispose or delete all Customer Data within a commercially reasonable time period when it is no longer needed for the purpose for which it was obtained. Customer must inform PowerSchool when Customer Data is no longer needed. Disposition will include (1) the shredding of any hard copies of any Customer Data; (2) erasing ; or (3) otherwise modifying the personal information in those records to make the information unreadable or indecipherable by human or digital means. Nothing in this Agreement authorizes PowerSchool to maintain Customer Data beyond the time period reasonably needed to complete the disposition. Upon request by Customer, PowerSchool will provide written notification to Customer when all Customer Data have been disposed. Upon receipt of a*

[47] The email actually says August 31, 2021, which I assume is a typo.

> *request from Customer, PowerSchool will provide Customer return of Customer Data, within ten (10) calendar days of receipt of said request, as commercially reasonable. Customer acknowledges there may be a reasonable service fee attached to such data return service where more than two (2) such service request is submitted by the Customer during the term. PowerSchool will promptly provide a copy of the Customer Data in PowerSchool's possession at termination or expiration of the Agreement and will certify in writing delivery to Customer.* [Bolding in original]

[160] Clause 2.3 addresses disposal on termination. It states:

> *Complete Disposal Upon Termination of this Agreement. Upon termination of this Agreement, PowerSchool will dispose of or delete all Customer Data within a commercially reasonable time period following termination; provided, however, in no event will PowerSchool dispose of Customer Confidential information pursuant to this provision unless and until PowerSchool has received affirmative written confirmation from Customer that Customer Data needs not be transferred to a separate account.*

[161] "Customer Data" is defined at clause 1.4 of the 2021 MSA as "all data, files, documents and records uploaded to a PowerSchool Subscription Service or transmitted to PowerSchool under this Agreement for or on behalf of the Customer. Customer Data is the property of the Customer". This definition includes any personal information provided to or otherwise stored in PowerSchool's software application. "Customer Confidential Information" is defined in the Proprietary Rights clauses in clause 3 of the MSA. In clause 3.3 it is defined as "any Customer Data belonging to Customer, or any other Customer information or data labelled or identified as confidential at the time of disclosure…" It is unclear whether personal information is included within this definition.

[162] Based on the facts presented by the School Division, there appears to have been a misunderstanding between the parties on a number of fronts.

[163] The letter sent March 5, 2021, by the School Division sets out that it is terminating its PowerSchool contact effective August 31, 2021. There is no mention in this letter as to what is to happen with the School Division's personal information stored in PowerSchool's software application.

[164] The email from PowerSchool on August 25, 2021, confirms that the contract term date ends on August 31, 2022, not 2021. It is unclear if this is a typo, although I assume it is and should have said August 21, 2021. There is no mention in this email about what will happen with the School Division's personal information stored in PowerSchool's software application.

[165] On July 8, 2022, the School Division emails PowerSchool asking why its instance of the SIS is still live and expressly requests that the data be purged "following your regular data retention policies". It is unclear what data retention policies are being referred to.

[166] On July 21, 2022, PowerSchool responded confirming that the decommissioning of the SIS had been completed and will no longer be available. There is no mention of what will happen with the School Division's personal information stored in the PowerSchool software application or a response regarding the reference in the email to "data retention policies".

[167] The facts show that neither party properly addressed the deletion of this personal information from PowerSchool's software application as set out in clauses 2 or 2.3 in the agreement.

[168] It is clear that the School Division was of the view that its personal information had been deleted, given its surprise on being notified that this information was involved in the Incident. It is unclear

why the PowerSchool representatives did not address the School Division's personal information during the termination discussions in 2021 given its responsibility under clause 2 which requires it to "promptly provide a copy of the Customer Data in PowerSchool's possession at termination or expiration of the Agreement" and to certify it has done so in writing to the Customer, and its duty under clause 2.3 to delete or dispose of Customer Data "within a commercially reasonable time period following termination".

[169] It is also clear that the personal information was not deleted or disposed of given that the School Division was able to access the information through its SIS instance in 2024 that was never decommissioned as represented by PowerSchool in 2021.

[170] While it is clear from the facts that the School Division's instance of the SIS has now been decommissioned, it remains unclear whether the School Division's personal information has been securely deleted or disposed of. This matter remains outstanding.

[171] I note here that the process of termination and deletion or destruction of personal information stored in PowerSchool's software applications has proven problematic for some of its customers. For example, in Investigation Report 003-2025, 035-2025 Prairie Spirit School Division (PSSD), it was identified that PowerSchool failed to decommission PSSD's SIS instance, which PSSD had terminated in 2022. In January 2024, PSSD discovered that the instance was still live. There was also an issue with having the personal information of this School purged despite PSSD's attempts to do so. The personal information of PSSD's students, staff and parents was also involved in the Incident. This is similar to what happened in the case of the School Division.

[172] Retention and destruction policies and processes are an essential component of personal information security given the risks of retaining personal information beyond that which is necessary, as determined by law or business needs. Failure to adhere to these policies and processes, or as here, the requirements in the 2021 MSA and DPS, creates risks to individuals. As happened here, the individuals whose personal information should have been deleted from PowerSchool's software applications prior to the Incident, but due to inadequate disposition and deletion practices by PowerSchool was not, had their personal information exfiltrated by a malicious actor thereby causing them a real risk of significant harm.

[173] The Public Bodies all identified having retention schedules for the personal information of students. This is because of the Student Record Regulation under the *Education Act*. This regulation sets out in section 4(1) the retention requirements for student records[48].

- It requires the student record to be retained for 7 years after the student/child ceases to attend a school operated by the board.
- For a student that transfers from an Alberta school to an extra-provincial one, it requires the student record to be retained for 7 years after the date the student would have been expected to complete grade 12.
- It permits retention of the student record for a longer period if authorized by a resolution of the board.

[48] Defined therein in section 2(1) as "all information affecting the decisions made about the education of the student or child that is collected or maintained by a board and includes specific information as set out in paragraphs (a) through (t) thereunder.

[174] As can be seen by what happened here, it is imperative that the Educational Bodies securely dispose of or destroy personal information of its students once the retention period expires, including that information which may be stored in PowerSchool's software applications.

Conclusion about decommissioning an instance of SIS on termination

[175] Based on the foregoing, I conclude that PowerSchool did not follow its agreed upon terms for decommissioning this School Division's instance of PowerSchool and securely delete the Personal Information as required by its agreement. This falls below the standard required by section 38 of the FOIP Act to reasonably secure the Personal Information, as retention and destruction of personal information forms part of these security requirements that this School Division is bound to comply with. It is unfortunate that, as a result of these failures by PowerSchool, the Personal Information of this School Division was involved in the breach when it should not have been.

Issue Finding

[176] For the foregoing reasons, I find that the Educational Bodies did not meet their respective obligations under section 38 of the FOIP Act as it relates to the protection of the Personal Information involved in the Incident:

(a) as a result of not having adequate policies and procedures in place to meet their respective duties under section 38; and

(b) as a result of the deficiencies in PowerSchool's security measures which led or otherwise contributed to the compromise of the Personal Information involved in the Incident:

i. failure to adequately identify and address the risks of the remote access for support functions;

ii. failure to develop, implement and enforce an access control policy that meets industry standards for all levels of administrative level or privileged accounts;

iii. failure to implement and use multi-factor authentication to access PowerSource and the SISs;

iv. failure to develop, implement and enforce strong password policies;

v. failure to harden applications by removing default features not needed, including disabling the always on remote access feature in SIS that led to persistent remote maintenance connections;

vi. failure to identify security vulnerabilities in PowerSource, by failing to classify PowerSource as a critical resource for the purpose of security assessments;

vii. failure to decommission and securely delete data as required under contractual agreements;

viii. failure to securely segregate network infrastructures that host PowerSource and SIS;

ix. failure to notify Educational Bodies of the Incident in accordance with the terms of agreement with those Bodies.

Educational Bodies' Representations to Issue Finding

[177] In representations made by one Educational Body to the Preliminary Investigation Report, it submitted that it "fulfilled its **duty to protect personal information** by making **reasonable security arrangements** pursuant to **section 38 of the *Freedom of Information and Protection of Privacy Act* (FOIP Act)** through the establishment and maintenance of robust contractual agreements aligned with established guidance for managing service providers" [bolding in original]. It added that its "methodology for ensuring compliance with Section 38, particularly in engaging PowerSchool as a service provider (deemed an "employee" under the FOIP Act), rigorously followed the critical provisions outlined in the *Contract Managers Guide* [sic] and relevant best practices." In pointing to the guidance contained in the Contract Manager's Guide to FOIP and Records Management (Guide),[49] it set out the clauses in its agreement with PowerSchool that align with the guidance provided in the Guide, highlighting that these clauses are evidence that in this case it met its section 38 obligations as it pertains to vendor management and reasonable security. There is one representation suggesting that it is sufficient for the contract to reference other legal frameworks and to infer therefrom that the protections set out in the agreement would align with the obligations in the FOIP Act. More on this below.

[178] As indicated at paragraphs 44 and 45 of this Investigation Report, I acknowledged that the agreements, on their face, appeared to meet the section 38 requirements, and for this reason it was reasonable for the Educational Bodies to rely on the security measures set out therein as sufficient to meet their section 38 requirements. However, as was found, PowerSchool's security measures fell below the section 38 requirements because their practices, as set forth in the agreements, as indicated herein, fell below the standards articulated in the agreements.

[179] Because under the FOIP Act, PowerSchool is a deemed employee of the Educational Bodies, it is these bodies, not PowerSchool, that are ultimately accountable for compliance with section 38. Representations in a contract alone are not enough to meet the section 38 requirements when engaging a service provider to perform activities involving personal information that is in a public body's custody or control. Public bodies must take the extra step of satisfying themselves that the service provider actually has these measures in place, the measures are working as expected and are maintained throughout the term of the contract. This is why it is necessary to also have policies and procedures concerning vendor management to ensure all aspects of outsourcing activities are managed such that they will meet the section 38 obligations. As was also found, the majority of public bodies did not have adequate policies and procedures, including for vendor management, in place to meet their section 38 obligations.

[180] I will add here that ensuring the adequacy of security measures, whether internal or external, rests with public bodies under the FOIP Act. Just because a public body outsources certain of its activities does not outsource its accountability as it relates to personal information. The requirements in the FOIP Act cannot be contracted out of. Any public body using vendors as part of its programs, activities, or services that involve personal information must oversee the security of its vendor the same as it would its own internal security.

Lack of FOIP Act mentioned in agreements with PowerSchool

[181] In this same Educational Body's representation regarding contractual provisions needed to meet the section 38 requirements, adjacent to the requirement to "stipulate contractor is accepting the

[49] Published by the Government of Alberta.

same responsibilities" it says "PowerSchool's contractual adherence to industry standards and legal requirements (such as FERPA Canadian Privacy Act, and PIPEDA) ensured they contractually accepted responsibilities commensurate with our obligations under Part 2 of FOIP Act". I disagree with this conclusion for the following reasons.

[182] Having reviewed all the agreements provided by the Educational Bodies, not one referenced Alberta's FOIP Act. There was one version that referenced Ontario's public sector privacy law.

[183] The referenced *Family Educational Rights and Privacy Act* (FERPA) is a US federal law that regulates access and disclosure of student education records[50]. This is not a privacy law that would be equivalent in any way to any of Canada's privacy laws. Canada's *Privacy Act* is a federal law that regulates the personal information of Canada's federal public sector and differs substantially from other Canadian jurisdictions' privacy laws. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to the private sector and has an entirely different legal framework than that which exists in the FOIP Act, which is a public sector privacy law[51]. Several of Ontario's laws are included in the 2021 agreement including its *Freedom of Information and Protection of Privacy Act*, which also differs from Alberta's FOIP Act in many respects. As such, reference to these laws has no bearing on whether the privacy protections and security measures in the FOIP Act would be met. It is up to the Educational Bodies to ensure that the correct legal framework is referenced and applied in its contractual provisions.

Corrective actions taken by Educational Bodies since the investigation

[184] In its representations, one Educational Body indicated that it "acknowledges the findings outlined in the Preliminary [Investigation] Report and accepts that the PowerSchool incident revealed opportunities for improvement both within our internal privacy framework and in the oversight of third party service provider." It then listed out numerous measures it has since implemented, such as, strengthened: vendor and system access controls, network and infrastructure security, monitoring and detection, data management and privacy, incident response and communication, and student information system access management.

[185] Another Educational Body stated that it "remains committed to continuous improvement in privacy management, adding that it "will review our procedures, contracts, and administrative practices to ensure they reflect the Commissioner's guidance and the evolving expectations under POPA, including with our development of a Privacy Management Plan".

Corrective actions taken by PowerSchool since the investigation

[186] In its representations to the Preliminary Investigation Report, PowerSchool included a number of corrective actions it has taken since the investigation, which are as follows:

[50] https://studentprivacy.ed.gov/faq/what-ferpa.

[51] This is referenced in the 2024, 2022 and 2021 agreements.

1. Leveraging multi-factor authentication

- Enforced multi-factor authentication (MFA) for all product access by Company personnel, including SIS access via VPN or SSO, and deployment of MFA-protected virtual desktop images for any personnel not on company laptops

- Migration of the maintenance access function from PowerSource to an Azure-based platform leveraging Microsoft Entra for identity and access management with mandatory SSO and MFA

2. Hardening maintenance remote access

- Removal of the “always on” maintenance access option for SIS customers, and limitation of maintenance access duration to no more than 30 days, with the duration set by the customer’s SIS administrator

3. Tightening access controls

- Implementation of a three-tier internal approval process for maintenance access and more granular, role-based access (e.g., view-only and support-desk roles) to reinforce least-privilege principles

4. Retraining SIS maintenance staff

- Retraining of all staff with maintenance access to SIS

5. Enhancing suspicious activity monitoring

- Deployment of new detections and alerting for suspicious activity, including alerts based on PowerSource access logs directed to the Security Operations Center for investigation and escalation

6. Enhancing security incident reporting

- Establishment of a Security Concerns ticket mechanism to streamline reporting of potential security issues across the organization

7. Strengthening information security governance

- Expansion of the information security organization, including the addition of Business Information Security Officers and Identity and Access management roles

In response to our questions of May 2025, PowerSchool provided the following information about decommissioning and deletion of personal information from the SIS instances.

8. Developing and implementing a new decommission policy

- In regard to why PowerSchool had failed to securely remove its clients' information from instances of SIS for clients who had terminated their agreement with PowerSchool, PowerSchool stated:

  > *Before the December 2024 cybersecurity Incident, PowerSchool had not yet removed all customer data from PowerSchool's systems for certain former customers due to unintentional implementation gaps.*

- PowerSchool further stated that it has created a new Decommission Policy that includes processes to provide its customers with the option to receive a copy of their data and steps that PowerSchool will take to delete customer data in the event that PowerSchool's attempts to communicate with the customer regarding its intention to delete the data fail.
- A copy of the policy was provided to the OIPC by PowerSchool and includes a requirement to complete a certificate of data destruction, which will be issued to the customer and retained by PowerSchool in the customer's record. A sample of the certificate of destruction was provided to the OIPC.

Protection of Privacy Act or "POPA"

[187] On June 11, 2025, POPA was proclaimed in force and the FOIP Act was repealed. As of this date, POPA applies to the Educational Bodies.

[188] POPA is a modernized privacy law that was designed to strengthen privacy protection in Alberta. There are several requirements in POPA that the Educational Bodies must comply with as it relates to the security and protection of personal information in their respective custody or control, including the Personal Information involved in the incident. I have set out the relevant provisions of POPA and its regulations below.

Protecting personal information

[189] Section 10(1) of POPA sets out the duties of public bodies as it relates to protecting personal information.

> ***10(1)*** *The head of a public body must protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.*

[190] Section 1(2) of the Protection of Privacy Regulation[52] defines the meaning of "reasonable security arrangements" in section 10(1) of POPA.

> ***1(1)****For the purposes of the Act*
>
> > *(c) "reasonable security arrangements" means administrative safeguards, physical safeguards and technical safeguards to protect personal information, data derived*

[52] Alberta Regulation 132/2025.

> *from personal information and non-personal information in the custody or under the control of a public body that*
>
> *(i) are appropriate and proportional with the security classification level of the information or data, and*
>
> *(ii)…*
>
> ***(2)** For the purposes of subsection 1(c)*
>
> *(a) "administrative safeguard" means a policy or procedure or practice to manage a public body's conduct that protects the privacy of personal information, data derived from personal information and non-personal data;*
>
> *(b) "physical safeguard" means …*
>
> *(c) "technical safeguard" means a measure to protect a public body's electronic information and control access to it".*

[191] The Protection of Privacy (Ministerial Regulation)[53] establishes the following requirements concerning the public body's duties under section 10(1) of POPA.

> ***Security classification levels***
>
> ***2(1)** A public body must assign a security classification level to all personal information, data derived from personal information and non-personal data in the custody or under the control of the public body, based on an internal classification system established by the public body.*
>
> ***(2)** The security classification level assigned to personal information must reflect the sensitivity of the personal information.*
>
> ***Security arrangements and validation measures***
>
> ***3(1)** The reasonable security arrangements that a public body must make to protect personal information, data derived from personal information and non-personal data against such risks as unauthorized access, collection, use, disclosure or destruction must be appropriate and proportional with the security classification level of that information or data.*
>
> ***(2)…***

[192] Section 1 of the Ministerial Regulation establishes that the following personal information is deemed to be of "high sensitivity":

> *(a) biometric information about an identifiable individual;*
> *(b) financial information about an individual; and*
> *(c) **personal information respecting a minor**, senior or vulnerable individual. [Bolding mine]*

[53] Alberta Regulation 143/2025.

[193] Together, these provisions essentially codify the interpretation of “reasonable security measures” as described above for section 38 of the FOIP Act and clarify that personal information respecting a minor is of high sensitivity. This means that a public body that has custody or control of this type of personal information must protect it at a level commensurate with its classification as highly sensitive. This would require advanced security measures for its protection and include written policies, procedures or practices. Any agreement with PowerSchool concerning any personal information respecting a minor must reflect these new requirements to ensure compliance with section 10(1) of POPA and its regulations as applicable. POPA must be referenced in the agreement as the law applicable to any personal information collected, used, disclosed or accessed by PowerSchool as it is this law that sets the privacy and security standards that PowerSchool must comply with as a deemed employee of the Educational Bodies under POPA.

Mandatory breach reporting

[194] Section 10(2) of POPA establishes a duty for public bodies to notify individuals if there is a real risk of significant harm to an individual or individuals from a breach. Public bodies must also report the breach to the Commissioner and the Minister responsible for POPA.

> ***(2)*** *If an incident occurs involving the loss of, unauthorized access to or unauthorized disclosure of personal information in the custody or under the control of a public body where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss, unauthorized access or unauthorized disclosure, the public body must give notice, without unreasonable delay, of the incident to the following:*
>
> *(a) the individual to whom there exists a real risk of significant harm;*
> *(b) the Commissioner;*
> *(c) the Minister.*
>
> ***(3)*** *A notice given under subsection (2) must comply with the prescribed requirements.*

[195] Section 4 of the Protection of Privacy (Ministerial) Regulation establishes criteria for determining whether there is a real risk of significant harm, which triggers the section 10(2) duty to notify and report a breach as indicated under that section. Section 4 also specifies what must be in a notice to an affected individual and in the reports provided to the Commissioner and Minister about the breach.

[196] This duty will require the Educational Bodies to ensure there are adequate clauses in the agreement with PowerSchool to ensure they are able to meet this duty should another breach of personal information at PowerSchool occur.

Privacy Management Programs

[197] Section 25 of POPA requires a public body to develop, implement and maintain a privacy management program.

> ***25(1)*** *A public body must establish and implement a privacy management program consisting of documented policies and procedures that promote the public body's compliance with its duties under this Act.*
>
> ***(2)*** *A privacy management program must*
>
> > *(a) be proportional to the volume and sensitivity of the personal information in the custody or under the control of the public body, and*
> >
> > *(b) comply with the prescribed requirements.*
>
> ***(3)*** *Any person may request a copy of a public body's privacy management program, and the public body must provide the person with a copy, or with directions to where the person may access a copy, within 30 business days of the request.*
>
> ***(4)*** *A request made and the public body's response under subsection (3) must comply with the prescribed requirements.*
>
> ***(5)*** *Notwithstanding subsections (1) and (3), a public body is not required to do the following until one year after this section comes into force:*
>
> > *(a) establish and implement a privacy management program;*
> >
> > *(b) provide a person with a copy of its privacy management program or with directions to where the person may access a copy.*

[198] Section 6 of the Protection of Privacy (Ministerial) Regulation sets out what a privacy management program must include.

> ***6(1)*** *A privacy management program established by a public body under section 25 of the Act must include*
>
> > *(a) the designation or identification of a privacy officer within the public body who is responsible for ensuring the public body's compliance with the Act,*
> >
> > *(b) internal policies and procedures to address the public body's duties under the Act, including policies and procedures for*
> >
> > > *i. responding to*
> > >
> > > > *(A) requests for the correction of an individual's personal information under section 7 of the Act,*
> > > >
> > > > *(B) incidents described in section 10(2) of the Act, and*
> > > >
> > > > *(C) complaints made under section 38(2) of the Act,*
> > >
> > > *ii. the creation, use and disclosure of non-personal data, if the public body will create, use or disclose non-personal data, and*

iii. how automated systems will use personal information, including any security or technical safeguards that will be implemented to protect personal information, if the public body will use personal information in an automated system to generate content or make decisions, recommendations or predictions,

(c) the establishment of a security classification system for personal information, data derived from personal information and non-personal data in the custody or under the control of the public body,

(d) mandatory training for employees of the public body about the obligations of those employees under the Act, with specified expiry periods after which retraining is required, and

(e) timelines for the periodic review, assessment and update of the privacy management program.

(2) *If a public body has custody or control of a high volume of personal information or highly sensitive personal information, the public body's privacy management program must also include the following:*

(a) documentation of the public body's internal privacy management structure and internal policies and procedures to address the public body's duties under the Act, which must address

i. the roles, responsibilities and accountabilities of employees of the public body in relation to the public body's obligations under the Act,

ii. the public body's process for completing and submitting privacy impact assessments,

iii. the public body's policies and procedures for proactive monitoring of information systems that hold personal information, data derived from personal information or non-personal data, to assess security measures and mitigate risks,

iv. the public body's policies and procedures related to oral, electronic and written consent, and

v. the public body's policies related to the use of personal information in artificial intelligence systems, the creation of data derived from personal information and the creation of non-personal data, if the public body is using personal information in artificial intelligence systems, the creation of non-personal data or data matching activities;

(b) written administrative, technical and physical safeguards for managing personal information, data derived from personal information and non-personal data.

(3) *Each public body must establish a process for making the public body's privacy management program available to the public on request or must make the public body's privacy management program publicly available on the public body's website.*

> ***(4)*** *When making a public body's privacy management program available to the public, a public body may withhold technical information, security-related information and other information that could compromise the security of personal information in the custody or under the control of the public body.*

Privacy Impact Assessment

[199] Section 26(1) of POPA requires public bodies to prepare a privacy impact assessment in prescribed circumstances and, if required by regulations, submit it to the Commissioner in accordance with the regulations. Section 26(2) sets out that a privacy impact assessment must:

> *(a) identify and review risks associated with the public body's collection, use and disclosure of personal information,*
>
> *(b) develop mitigation strategies and safeguards respecting those risks,*
>
> *(c) address how the public body will comply with its duties under this Act, and*
>
> *(d) comply with the prescribed requirements.*

[200] Section 27(j) authorizes the Commissioner to request a copy of the privacy impact assessment of a public body, and 26(3) requires a public body to provide the Commissioner with a copy of the same within 30 days of the request.

[201] Section 7 of the Protection of Privacy Act (Ministerial) Regulation establishes the circumstances requiring a public body to prepare a privacy impact assessment and what it must contain.

> ***Privacy impact assessments***
>
> ***7****(1) A public body must prepare a privacy impact assessment under section 26 of the Act with respect to a new, or a substantial change to an existing, administrative practice, program, project or service that will involve the collection, use or disclosure of personal information if one or more of the following apply:*
>
> *(a) the loss of, unauthorized access to or unauthorized disclosure of the personal information could result in significant harm as determined in accordance with section 4;*
>
> *(b) one or more of the factors requiring the submission of a privacy impact assessment to the Commissioner established by subsection (5) apply.*
>
> ***(2)*** *A privacy impact assessment must*
>
> *(a) include a summary of the purpose of the collection, use or disclosure of personal information for the new, or a substantial change to an existing, administrative practice, program, project or service,*
>
> *(b) identify the types of personal information that will be collected, used or disclosed and reasonable security arrangements in place to protect that personal information,*
>
> *(c) identify the legal authority for the collection, use or disclosure of the personal information,*

> (d) *identify any privacy risks and mitigation strategies respecting the personal information,*
>
> (e) *identify any administrative, physical or technical safeguards in place to protect the personal information, including how the personal information will be securely transmitted, matched or linked by the public body, if applicable,*
>
> (f) *describe accuracy, correction and retention procedures that will be implemented to ensure the personal information is accurate and complete, and*
>
> (g) *establish a clear governance structure respecting the responsibilities and accountability of each public body if 2 or more public bodies are engaging in a common or integrated program or service or if a public body is collecting personal information from another public body under section 17(3) of the Act for the purpose of carrying out data matching.*
>
> ***(3)*** *A privacy impact assessment must provide a level of detail commensurate with the complexity of the practice, program, project or service the privacy impact assessment relates to.*
>
> ***(4)*** *Despite subsection (1),*
>
> (a) *in the case of a substantial change to an existing administrative practice, program, project or service, if a public body has previously completed a privacy impact assessment relating to the practice, program, project or service, the existing privacy impact assessment may be amended to account for the change to the practice, program, project or service provided that the amended privacy impact assessment complies with the Act and this regulation, and*
>
> (b) *in the case of a common or integrated program or service or data matching between 2 or more public bodies, the public bodies involved in the common or integrated program or service may prepare a joint privacy impact assessment and each public body must prepare an addendum to address any unique collection, use or disclosure circumstances that apply to that public body.*

[202] Section 7(5) sets out when a privacy impact assessment must be submitted to the Commissioner for review and comment.

> ***(5)*** *A privacy impact assessment must be submitted to the Commissioner if one or more of the following factors apply:*
>
> (a) *a practice, program, project or service will collect, use or disclose personal information deemed to be of high sensitivity;*
>
> (b) *a practice, program, project or service will involve the personal information of a significant percentage of the population the public body serves;*
>
> (c) *a practice, program, project or service will involve data matching between 2 or more public bodies;*
>
> (d) *a practice, program, project or service is part of a common or integrated program or service;*
>
> (e) *a practice, program, project or service involves the development or use of innovative technology;*

> *(f) the Commissioner requests a copy of a privacy impact assessment under section 27(1)(j) of the Act.*
>
> ***(6)** If a public body is required to submit a privacy impact assessment under subsection (5) and the Act or this Regulation requires the public body to enter into an agreement relating to the practice, program, project or service the privacy impact assessment relates to, the portions of the agreement relating to the protection of privacy must be submitted to the Commissioner together with the privacy impact assessment.*

Recommendations

Preface

[203] Before making my recommendations, I would like to acknowledge the following representations made by four of the Educational Bodies that are relevant to my recommendations.

- *Finally, we would also like to remind the AB OIPC that PowerSchool is an international business, supporting over 60 million students and 18,000 customers across the planet (as indicated on their website). It is also one of the industry leaders in its field of activity and is used extensively across North America. Individual Educational Bodies represent a negligible proportion of PowerSchool's users, thereby greatly diminishing their ability to negotiate terms with PowerSchool or request changes to PowerSchool's internal policies and procedures. To the extent the AB OIPC expects Educational Bodies to be responsible for their service providers' compliance with statutory requirements, sufficient assistance from the provincial government, including Alberta Education, should also be provided to assist Educational Bodies in their compliance with statutory requirements. We assume this will be discussed by the AB OIPC in the forthcoming "Recommendations" section of its investigation report"*

- *In essence, we believe the AB OIPC's draft investigation report paints an incomplete picture of Educational Bodies' response to the incident, and does not properly address or outline Alberta Education's role in ensuring that personal information processed by Educational Bodies is adequately protected.*

- *That said,* [Educational Body] *wishes to highlight the practical limitations faced by school divisions in overseeing complex, cloud-based information systems operated by third-party vendors such as PowerSchool. While* [Educational Body] *accepts that it remains accountable under section 10 of POPA (formerly section 38 of FOIP), it does not have the technical capacity or legal authority to independently audit or inspect vendor systems, data centers, or network configurations.* [Educational Body] *therefore relies on contractual representations, industry certifications (such as SOC 2 or ISO 27001), and privacy schedules that bind service providers to the same standards required of public bodies.*

- *We respectfully submit that the standard of "reasonable measures" under section 38 must be interpreted in a manner that reflects the practical capabilities and control of public bodies in the K–12 education sector. Requiring individual school divisions to perform direct technical oversight of international cloud vendors would not be feasible or proportionate. A coordinated provincial or sectoral approach—such as Ministry-led vendor vetting or standardized privacy assurance* *frameworks—would better ensure consistent protection of student data across Alberta while recognizing the operational realities of school jurisdictions.*

[204] One of the Educational Bodies commented that "PowerSchool is the only option for the large boards to meet the obligations of Alberta Education in providing data to them, we are unable to provide this data in any other way".

[205] I would also like to acknowledge the actions taken by PowerSchool since the Incident, many of which are a step toward addressing the recommendations made to remedy the non-compliance found in this Investigation Report. I would further like to acknowledge steps taken by the Educational Bodies to better protect personal information when engaging vendors as part of their programs, activities or services.

[206] Lastly, POPA is now the law that applies to these Educational Bodies. This law, a modernized privacy law, requires public bodies to develop, implement and maintain a privacy management program as prescribed in the Act and regulations. It also requires public bodies to secure and protect personal information according to a specified scheme, which is significantly enhanced over that of section 38 of the FOIP Act. My recommendations take these new requirements into account.

[207] Below are my recommendations to remedy the non-compliance with section 38 of the FOIP Act by the Educational Bodies, to ensure compliance with POPA, and to mitigate the risk of a breach involving the Educational Bodies' instances of SIS, or other technology acquired by these bodies, in the future.

Recommendations to Educational Bodies

1) I recommend that within 6 months of receiving this Investigation Report, the Educational Bodies each develop and implement:

    (a) policies and procedures to meet their respective obligations under section 10(1) of POPA and its regulations including for vendor management and oversight more generally that ensures compliance with POPA and addresses the findings in this Investigation Report; and

    (b) breach management policies and procedures that meet the requirements of POPA for breach notification and reporting.

    I will note here that these are components of developing and implementing a privacy management program, which the Educational Bodies are required to establish and implement under POPA on or before June 11, 2026.

2) I recommend that the Educational Bodies work with my office on the development of these policies and procedures in recommendation 1.

3) I recommend that within 6 months of receiving this Investigation Report, the Educational Bodies develop standardized contract language to incorporate into any contract used to procure technology that ensures compliance with POPA and the respective Educational Body's policies and procedures.

4) I recommend that the Educational Bodies work with my office on the development of the standard contract language in recommendation 3.

5) I recommend that within 8 months of receiving this Investigation Report, the Educational Bodies prepare a privacy impact assessment in accordance with the requirements in POPA and the Protection of Privacy (Ministerial) Regulation for their respective instances of SIS and provide the same to the Commissioner for review and comment.

6) I recommend that within 60 days of receiving this Investigation Report, each of the Educational Bodies ensure that remote access for maintenance is disabled for their respective SIS instances and work with PowerSchool to ensure access is only enabled on-demand to perform maintenance and to ensure there is no persistent access.

Recommendations to PowerSchool

7) I recommend that PowerSchool harden its remote access feature to the Educational Bodies' instances of SIS:

   (a) using technical and administrative measures to ensure remote access is solely controlled by the Educational Bodies such that access by PowerSchool employees or contractors is only on-demand and terminated immediately after support is complete; and

   (b) to eliminate to the degree possible any persistent remote access feature.

8) I recommend that PowerSchool develop and implement a remote access solution comprising of policies and technology that meets industry standards.

9) I recommend that PowerSchool revise and enforce its Access Control Policy to address the risks associated with administrative level privileges such that it conforms with industry standards.

10) I recommend that PowerSchool implement the use of multi-factor authentication for access to the SIS instances via PowerSource.

11) I recommend that PowerSchool review, revise and enforce a Strong Password Policy to meet industry standards for passwords, including for password complexity including length, composition, expiration and rules regarding how many iterations are allowed before an old password can be re-used, as well as the use of compromised password checks.

12) I recommend that PowerSchool securely segment PowerSource and the SIS network environments by implementing additional controls that will prevent a threat actor from moving between the segmented environments.

13) I recommend that PowerSchool ensure that PowerSource be in scope for future security risk assessments.

14) I recommend that PowerSchool establish a decommissioning process that ensures any personal information stored in instances of SIS at termination of a contract with any Educational Body is removed from PowerSchool's systems within a reasonable period of time following the end of the contract.

15) I recommend that PowerSchool work with the Educational Bodies on preparing their respective privacy impact assessments.

16) I recommend that PowerSchool establish a mechanism to report to the Educational Bodies with active instances of SIS, at least annually, on the security measures used to protect the personal information stored therein that demonstrates compliance with the terms of the agreements with these Bodies concerning their respective instances of the SIS. Each report must also highlight any changes to the security measures.

17) I recommend that within 6 months of receiving this Investigation Report, PowerSchool provide me with evidence to satisfy me that recommendations 7 to 16 have been complied with.

18) I recommend that within 8 months of receiving this Investigation Report, PowerSchool work with the Educational Bodies to draft a new contract with PowerSchool for their respective instances of SIS that ensures compliance with POPA and addresses the findings herein.

19) I recommend that once the new contracts with the Educational Bodies have been finalized, within a reasonable time thereafter PowerSchool work with these bodies to enter into the new agreement.

[208] I recognize that PowerSchool has already made changes that may address some of the foregoing recommendations and I will consider the same as part of assessing the implementation of the recommendations on acceptance of them by PowerSchool.

Recommendations to Government

[209] Use of technology in the education sector (EdTech) is becoming more common. Use of this technology creates risks to children and youth whose personal information is processed and managed by educational staff and EdTech vendors. That is why I have as one of my goals in my Business Plan to identify, facilitate and support opportunities to enhance privacy protection for children and youth. Within this goal, I have identified the need to work with education partners in

the province who are using or intend to use EdTech in order to prevent harm that may occur to children and youth from the use of this technology.

[210] In my comments and recommendations for modernization of Alberta's privacy laws, I have consistently highlighted the importance of regulating to protect children's privacy in this digital age and have recommended specific protections for children be codified in all three Acts.[54]

[211] Commissioners across Canada and data protection authorities globally have been calling for better legal protection for children to mitigate the risks of harm to them as a result of their exposure to technology, which includes EdTech.

[212] In 2023, Canada's FPT privacy regulators issued a joint resolution calling on our respective governments to put the best interests of young people first by taking immediate action as necessary to:

- protect young people from commercial exploitation and the use of their personal information to negatively influence their behaviour or to cause them harm;
- promote the privacy rights of young people;
- review, amend or adopt relevant privacy legislation to be consistent with internationally-recognized policy and legal instruments to ensure adequate protection of the privacy rights of young people; and
- require private sector organizations that collect, use and disclose the personal information of young people to:
    - implement strong safeguards;
    - be transparent about these practices; and
    - enhance access to effective remedies for young people.

[213] What happened in this case demonstrates that the risks from using EdTech are significant and can be widespread. Here, just one cyber incident affected more than 500,000 of Alberta's students and millions of individuals globally. As can be seen by this investigation, the below-standard security practices of an EdTech vendor, which is used by the majority of educational bodies in Alberta, allowed a threat actor to access and exfiltrate the personal information of students and others from the Educational Bodies' instances of SIS.

[214] The comments made by four Educational Bodies highlight the significant challenges these Bodies face when acquiring EdTech, including in negotiating contracts that will enable them to meet their respective privacy law obligations. As was noted by one, schools require technology to, inter alia, comply with their reporting obligations to government. In addition, these Educational Bodies

[54] HIA, POPA and PIPA.

identified that they do not have the requisite skills needed to evaluate an EdTech vendor's security measures. Evaluating the information security policies, procedures, and practices of a third-party vendor requires a specific set of skills that Educational Bodies generally do not have. An essential part of vendor management is ongoing oversight to ensure the terms of the agreements, including for security, are being met, which can be time-consuming.

[215] Furthermore, educational bodies in Alberta are relatively small. Vendors of EdTech can be very large, as was the case with PowerSchool, which is worth more than $5 billion and operates globally. Consequently, these Bodies do not have the negotiating power to enter into agreements that are unique to the privacy and security obligations set out in Alberta's privacy laws. This leaves them in the difficult position of having to sign standard form agreements, which in many cases are designed to comply with laws in the US or elsewhere but not with Alberta's privacy laws, or not use the application, the latter of which in this digital age is not really an option.

[216] It is clear from this investigation that Alberta's educational bodies require assistance in managing their acquisition of technology used for education-related purposes and for ongoing vendor oversight.

[217] To that end and based on the foregoing, I recommend as follows:

1) Government consider utilizing its procurement power to procure EdTech on behalf of educational bodies in Alberta under agreements that will enable them to comply with Alberta's privacy laws.

2) Government consider investing, through grants, non-profit funding or otherwise, in the evaluation of technology to be used by Alberta's educational bodies, which must include:

    (a) evaluating the technology from a "privacy by design" perspective;

    (b) ensuring that in its use, educational bodies will be positioned to comply with the applicable privacy law, including for security; and

    (c) ongoing monitoring of the vendor's privacy and security practices for the life of the contract.

3) Alternatively, or until such an organization is in place and conducting EdTech evaluations as described in the prior recommendation, consider establishing a government program or activity that will conduct these evaluations and monitor for ongoing compliance.

[218] I acknowledge here that under POPA, educational bodies that are public bodies in Alberta are required to prepare a privacy impact assessment (PIA) that must include an assessment of the authority to collect, use, disclose and maintain security of personal information using technology and that this, together with the requirement to submit these PIAs to the Commissioner for review and comment, may address aspects of recommendations 2(a) and (b). However, ongoing

monitoring and procurement will not be addressed through the PIA requirements in POPA. Some schools in Alberta are private. There is no equivalent PIA obligation under PIPA.

Concluding Remarks

[219] This Commissioner-led investigation resulting from a large scale breach of students, teachers, and parents/guardians involving 33 educational bodies in Alberta and PowerSchool was complex and demanded a significant amount of time by representatives from all parties involved. I thank them for their cooperation.

Diane McLeod
Information and Privacy Commissioner