OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2026-001

May 11, 2026

Department of Education and Early Childhood Development

Summary: The Commissioner initiated an own-motion investigation into the PowerSchool privacy breach that affected the entire Newfoundland and Labrador school system. This breach compromised the personal information of both current and former students dating back to 1995, as well as their parents or caregivers, together with teacher personal information dating back to 2010.

This Report outlines our investigation, summarizes key facts, and presents the Commissioner's recommendations to the Department of Education and Early Childhood Development.

Statutes Cited: Access to Information and Protection of Privacy Act, 2015, SNL 2015, c A-1.2, section 64 (protection of personal information); Management of Information Act, SNL 2005, M-1.01, section 6 (system for management of information); Schools Act, 1997, SNL 1997, SNL 1997 c S-12.2.

Authorities Relied On: NL OIPC Reports: P-2023-001/PH-2023-002; Alberta OIPC PowerSchool Report: F2025-IR-02; Ontario IPC PowerSchool Report : MR25-00002 et al; Saskatchewan OIPC PowerSchool Report: 003-2025, 035-2025.

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

One of the key findings of this Report is that the PowerSchool breach impacted 285,158 individuals, and is the second largest cyberattack Newfoundland and Labrador has faced in a relatively short period of time, being eclipsed only by the 2021 cyberattack that impacted the province's health care system. In this case, the breach occurred because a hacker was able to take advantage of PowerSchool's inadequate security measures, which failed to protect the information of citizens of this province, as well as others across Canada and around the world.

The context of this breach, however, is that in a tech-dominated age, governments and public bodies around the world often find that our relationship with large multinational tech companies is not a level playing field especially in smaller jurisdictions. In the education system, we have PowerSchool and Google Classroom, players that are so dominant in the marketplace that the pull of their products and services is quite strong, and often there are few, if any, alternatives. It feels, at times, that these companies use their size and dominance as leverage against demands to strengthen privacy protections.

Despite this context, and the geopolitical pressures that are currently in play, it is essential that governments and public bodies act diligently to ensure that any contractual arrangements with these entities not only meet the minimum standards of the law, but also considers the long-term impact on public trust. Large breaches such as this one do real damage to that trust. The information impacted by the PowerSchool breach was the responsibility of the leaders of our education system to protect. If public bodies in Newfoundland and Labrador believe they need to outsource management of that data, it must be clearly understood that in doing so they do not outsource accountability.

When it comes to large multinational companies, smaller jurisdictions may need to work with larger provinces or we can strengthen our own procurement and privacy legislation to ensure third-party vendors take the protection of Newfoundlanders and Labradorians privacy seriously.

ACKNOWLEDGMENT

Our Office wishes to acknowledge the cooperative and transparent manner in which the Department of Education and Early Childhood Development engaged with us throughout its response to the PowerSchool privacy breach and during the course of our investigation. The Department provided timely updates, maintained open lines of communication, and responded promptly to requests for information necessary to support our investigative work. We recognize the significant effort undertaken by the Department to address the breach and appreciate its constructive and diligent approach, which assisted our Office in carrying out its oversight responsibilities effectively. Looking ahead, we hope that the recommendations contained in this Report will assist the Department in continuing to strengthen its practices. Our recommendations are aimed at reducing risk, enhancing accountability, and better protecting the personal information entrusted to the Department by students, families, and educators across the province.

EXECUTIVE SUMMARY

When Powerschool experienced a cyberattack, it affected Newfoundland and Labrador's entire K–12 education school system. What may be surprising to many reading this Report is that the impact extended far beyond the current generation of teachers, students, and parents or guardians. Teacher personal information in PowerSchool SIS dates back to 2010. Student personal information in PowerSchool SIS dates back further to 1995, meaning anyone who attended as a student or had a child in the K–12 educational system in Newfoundland and Labrador from 1995 onward likely had personal information taken in the PowerSchool breach.

This breach impacted students, parents/caregivers, and teachers. The personal information taken in the breach impacted 285,158 individuals consisting of former students (the majority of which are now adults), current students, former teachers, and current teachers. Personal information taken in the breach included a combination of the following depending on which group an individual is in:

Current or former students:

- name
- date of birth
- gender
- medical care plan (MCP) number
- contact information
- medical alert information
- custodial alert information
- discipline alert information
- parent/guardian contact information
- emergency contact information
- guardian information
- other related information
- social insurance number (SIN)

Current or former teachers:

- name
- home address
- personal email address
- personal phone number
- MCP number
- SIN
- date of birth

Given the significant number of Newfoundlanders and Labradorians affected by this breach, this Office initiated an own-motion investigation to determine whether the Department had appropriate security and information management practices in place at the time of the breach, and whether it took reasonable steps in responding to the breach.

While this investigation identified weakness and gaps in the contractual language of the Department's agreement with PowerSchool, these were not the main issue when it comes to the breach. In fact, several jurisdictions with stronger and more comprehensive contracts were similarly affected. The main issue was not what PowerSchool stated they would adhere to for privacy protections, but that in reality PowerSchool's practices fell well below the standards they had set out in their agreements.

This cyberattack specifically affected instances of PowerSchool SIS where an "always on" remote maintenance feature had been enabled; this critical vulnerability allowed continuous remote access through PowerSchool's online support portal, PowerSource. The Department's

instance of PowerSchool SIS also had this "always on" maintenance feature enabled at the time of the incident, and as a result, personal information relating to over 285,000 Newfoundlanders and Labradoreans was taken in this cyberattack.

During this investigation the Department acknowledged being unaware of the "always on" remote maintenance connection and also being unaware that PowerSource was not included in the scope of PowerSchool's third-party security assessments and testing. **Ultimately this Report finds that the Department did not implement adequate oversight measures to ensure that PowerSchool was meeting its contractual obligations or maintaining reasonable security measures**.

While this Report includes recommendations aimed at strengthening the contractual provisions in the agreement, even the most robust contract cannot safeguard personal information without active and ongoing oversight to ensure those obligations are being fulfilled. Accordingly, **this Report recommends not only enhancing the Department's contractual provisions to better support privacy protection, but also implementing regular, systematic monitoring measures to verify PowerSchool's compliance with those obligations.**

The following summarizes the oversight-related recommendations in the Report, namely for the Department to:

- include robust contract enforcement provisions to allow the Department to demand documented evidence from PowerSchool demonstrating its compliance with the terms and conditions of the agreement;

- review PowerSchool's security and information management policies and procedures and associated documentation to ensure they address identified vulnerabilities that contributed to the PowerSchool breach;

- take steps to standardize, define, and document its monitoring of security and auditing provisions under current and future agreements with PowerSchool, and obtain evidence of PowerSchool's fulfillment of its contractual obligations on an annual basis;

- follow up with PowerSchool to request information and evidence of actions PowerSchool committed to undertake as part of its Letter of Commitment with the Federal Privacy Commissioner's Office; and

- take action to enforce its contractual provisions with PowerSchool, in the event PowerSchool does not comply with its contractual obligations to protect and secure personal information it processes.

Overall this Report largely finds that the Department took reasonable steps in responding to the breach, making a number of recommendations aimed at improving the Department's information management practices and improving the clarity of future notification efforts. However, a small number of current students were identified by the Department as having potential SIN information impacted and the Department failed to directly notify those

individuals like it had with Teacher SIN information. This Report recommends the Department directly notify current students identified as having potential SIN information impacted.

Another key finding of this investigation concerns the Department's collection of student Medical Care Plan (MCP) numbers. During the investigation, **the Department confirmed that 244,917 student MCP numbers were included among the personal information affected by the breach. The majority of these records relate to inactive accounts belonging to students who are no longer part of the K–12 system (190,651 inactive accounts compared to 54,266 active accounts)**.

Historically, MCP numbers were used as student identifiers, a practice this Office had previously advised should cease. With the implementation of PowerSchool SIS in this province, all current and former students were assigned unique student identification numbers. Despite this change, the Department continued to collect and retain student MCP numbers.

During the investigation, the Department was asked to explain why student MCP numbers continued to be collected and retained, particularly given that access to emergency medical services in this province does not require an individual to possess or present an MCP number. **Ultimately, this Report concludes that the Department did not demonstrate that student MCP information is necessary for the delivery of educational programming or services. As a result, the Department's collection of student MCP information is not authorized under the Act.** To address the past and ongoing overcollection of student MCP information, this Report recommends that the Department:

- cease the collection, use, and disclosure of student MCP information; and
- destroy and permanently purge student MCP information from all student records.

THE POWERSCHOOL BREACH

PowerSchool SIS and PowerSource

[1] PowerSchool Group, LLC (**PowerSchool**) is a private company that offers education technology software designed to support K-12 schools. One of its products is the PowerSchool Student Information System (**PowerSchool SIS**); PowerSchool SIS is a system designed to help schools manage student data (including grades, academic progress, attendance records, schedules, etc.) and it also provides tools for communication between teachers, parents, and administrators.

[2] PowerSchool SIS is used by all schools in Newfoundland and Labrador, including all English public schools, Conseil scolaire francophone provincial de Terre-Neuve-Et-Labrador

("**CSFP**"), private schools, and Indigenous schools[1]. The Department of Education and Early Childhood Development[2] (the "**Department**") has a contractual agreement with PowerSchool for a singular cloud-based instance of PowerSchool for use by schools in the province. The Department uses PowerSchool SIS as a database for part of its K-12 student records, as well as high school certification records and services in the province. Personal information of current and former students, dating from 1995 to the present, are stored within the province's instance of the PowerSchool SIS. Similarly, the personal information of teachers, dating from 2010 to the present, is also contained within the province's instance of the PowerSchool SIS.

[3] PowerSource is an online customer support portal for PowerSchool products. Instances of PowerSchool SIS, including our province's instance, are integrated with this support application. According to PowerSchool, the PowerSource application can be used by educational bodies to request maintenance support and used by PowerSchool's support technicians to remotely connect to the PowerSchool SIS instance.[3] PowerSchool support technicians use credentials (username and password) to log in to the PowerSource online portal, remotely connect and gain access to the PowerSchool SIS database, and provide maintenance support.[4]

Exfiltration of PowerSchool SIS Data by Threat Actor

[4] PowerSchool provided a Crowdstrike Investigation Report to our Office and indicated that the incident occurred between December 19 and December 28, 2024. During this period, a threat actor used compromised credentials belonging to a PowerSchool contractor or subcontractor[5] with administrative-level privileges[6]. The threat actor was able to log into PowerSource, remotely connect to certain PowerSchool SIS instances, and exfiltrate data from the teacher and student tables. The teacher and student data from Newfoundland and Labrador's PowerSchool SIS instance was among the data taken by the threat actor.

---

[1] See **Appendix A** for a timeline summary of the implementation of PowerSchool in Newfoundland and Labrador.
[2] Formerly known as the Department of Education.
[3] F2025-IR-02 at paragraph 48.
[4] CrowdStrike Investigation Report at page 5.
[5] MR25-00002 et al at paragraphs 13-15.
[6] F2025-IR-02 at paragraph 6.

[5] On December 28, 2024, PowerSchool became aware of the incident. Upon discovery, PowerSchool initiated its cyber security incident response protocol and organized a cross-functional response team, including third-party cyber security experts, to contain the threat and determine the scope of the cyberattack[7].

[6] On January 7, 2025, PowerSchool provided notice to the Government of Newfoundland and Labrador (**GNL**) that PowerSchool had experienced a cyber security incident. Upon receipt of this notice, GNL initiated its incident response processes for cyber and privacy investigations.

Ransom Payment and Continued Extortion Attempts

[7] Although PowerSchool paid a ransom after receiving assurances and evidence from the threat actor that the stolen data would be destroyed, the information was not deleted. On May 7, 2025, PowerSchool announced that school districts were receiving extortion attempts, using data taken during the December 2024 privacy breach.

[8] While other school districts in Canada did receive payment demands in May of 2025[8], as part of our Office's investigation, the Department confirmed it found no evidence of any similar attempts directed at schools in Newfoundland and Labrador.

Criminal Charges and Sentencing

[9] On May 20, 2025, the United States Attorney's Office for the District of Massachusetts announced[9] that a 19-year-old university student in Worcester, Massachusetts, had been charged "in connection with hacking into the computer networks of two U.S.-based companies and extorting the companies for ransoms". Court filings described one company as being "...a software and cloud storage company that served school systems in the United States, Canada, and elsewhere"[10] and this impacted company was later identified in media articles as being

---

[7] MR25-00002 et al at paragraphs 16.
[8] MR25-00002 et al at paragraphs 22.
[9] Press Release of United States Attorney's Office, District of Massachusetts.
[10] Information – United States District Court, District of Massachusetts.

PowerSchool[11]. According to the news release[12], the student demanded ransom payment of approximately $2.85 million in Bitcoin, with the threat that the personal information of over 60 million students and 10 million teachers would be leaked worldwide if not paid.

[10] On October 14, 2025, a United States District Judge in Worcester, Massachusetts sentenced the student hacker to four years in prison after finding him guilty of cyber extortion conspiracy, cyber extortion, and unauthorized access to protected computers.[13]

Privacy Commissioner of Canada Investigation of PowerSchool

[11] On February 11, 2025 the Privacy Commissioner of Canada announced the launch of an investigation under the **Personal Information Protection and Electronic Documents Act** relating to the PowerSchool breach.

[12] On July 22, 2025 the Privacy Commissioner of Canada issued a statement stating in part:

> In light of the actions that PowerSchool has already implemented, and those that it will implement over the coming months, Privacy Commissioner of Canada Philippe Dufresne has decided to discontinue the investigation that he launched in February but will be monitoring to ensure that all of PowerSchool's commitments are fully met.

[13] On July 15, 2025 the private company PowerSchool signed a Letter of Commitment in which PowerSchool agreed to a variety of commitments.

Breach Impact in Newfoundland and Labrador

[14] This breach affected Newfoundland and Labrador's entire K–12 education school system. What may be surprising to many reading this Report is that the impact extended far beyond the current generation of teachers, students, and parents or guardians. Teacher personal information in PowerSchool SIS dates back to 2010. Student personal information in

---

[11] See CBC News Article.
[12] Press Release of United States Attorney's Office, District of Massachusetts.
[13] United States District Court, District of Massachusetts Docket Number 4:25-cr-40015 (D. Mass. Oct 14, 2025) ECF: No. 22; See other related judgments at: No. 20, and No.21.

PowerSchool SIS dates back further to 1995, meaning anyone who attended as a student or had a child in the K–12 educational system in Newfoundland and Labrador from 1995 onward likely had personal information taken in the PowerSchool breach.

[15] **The PowerSchool breach impacted 285,158 individuals and is the second largest cyberattack Newfoundland and Labrador has faced in a relatively short period of time, being eclipsed only by the 2021 cyberattack that impacted our health care system.**

OIPC DECISION TO INVESTIGATE POWERSCHOOL BREACH

Jurisdiction

[16] The Commissioner has jurisdiction and authority under the **Access to Information and Protection of Privacy Act, 2015** (the "**Act**") to investigate privacy breaches involving public bodies. The Department is a public body and is therefore the respondent in this investigation.

Scope

[17] Although the Conseil scolaire francophone provincial de Terre-Neuve-et-Labrador (the "**CSFP**") is a separate public body under the Act, it is the Department that holds the contract with PowerSchool, and that provides direction on all PowerSchool-related matters to the CSFP, as well as private schools and Indigenous schools. Given the Department's ownership and control over the PowerSchool contract and program, we determined that the investigation should be focused solely on the Department.

Launch of Investigation

[18] On January 8, 2025, the Department reported this privacy breach to the Office of the Information and Privacy Commissioner ("**OIPC**") as required by section 64(4) of the Act.

[19] On May 30, 2025[14], OIPC provided notice to the Department that we were launching an own-motion privacy complaint investigation pursuant to section 73(3) of the Act.

[14] On May 30, 2025, OIPC also issued a news release regarding this investigation.

[20] On May 30, 2025, OIPC provided public notice of its decision to investigate the PowerSchool breach by issuing a news release which included commentary on the Commissioner's reasons for launching the investigation at that time:

> This breach involved MCP numbers, social insurance numbers, health details, and other sensitive information about current and former students and teachers in this Province going back a number of years. Before launching this investigation I felt it was appropriate to give the Department sufficient time to assess the impact of the breach, notify those who were impacted, and take steps to adjust its policies and practices. It has now had ample opportunity to do so.
>
> We have been in communication with the Department since receiving notification of the breach and we understand that the Department has already taken a number of positive steps. The purpose of my investigation is not only to assess whether the Department has responded adequately to the breach, but also to ensure that measures taken by the Department to prevent future occurrences of this nature are sufficient. People have a right to expect that when a public body collects their sensitive personal information that it will do so in accordance with the law. That means that a public body shouldn't collect more personal information than necessary, that it will take reasonable steps to protect the information it holds, and that it will retain that information for only as long as needed and then securely destroy it.

ISSUES

[21] Our investigation focused on the following two issues:

Issue 1: Security and Information Practices

Did the Department have reasonable security and information practices in place at the time of the PowerSchool breach as required by the Act?

Issue 2: Response to the Breach

Did the Department take reasonable steps in responding to the PowerSchool breach as required by the Act?

ISSUE# 1: SECURITY AND INFORMATION PRACTICES

Legislation

[22] Public bodies, including the Department, are required to have reasonable security and information practices in place to protect personal information in their custody or control. Section 64(1) of the Act states:

> 64(1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that
>
> (a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;
> (b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and
> (c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.

[23] The Act does not prescribe what specific security and information practices must be implemented. As indicated in OIPC's guidance on reasonable safeguards, an assessment of whether a public body has taken steps that are reasonable in the circumstances involves examining the security measures in place at the time of the breach. Whether such measures were reasonable will depend on contextual factors, including foreseeability of the breach, seriousness of potential harm, cost of preventative measures, and relevant standards of practice.

Agreements with Third-Party Service Providers

[24] Although a public body is permitted to use third-party service providers under the Act, the public body remains ultimately responsible for ensuring that reasonable security measures are implemented to safeguard against unauthorized access to personal information within its custody or control. This means that when a public body enters a contract with a third-party service provider, the contract must include terms that, if followed, will support the public body's compliance with the Act, as well as terms that will enable a public body to monitor the third-party's compliance with the contract.

[25] The Ontario Information and Privacy Commissioner has released guidance titled Privacy and Access in Public Sector Contracting with Third Party Service Providers. Although our

legislation is not identical to Ontario's, this guidance may serve as a useful framework to our province's public bodies that engage third-party service providers as it may assist them in addressing the privacy and access obligations under our own Act.

[26] The Ontario IPC PowerSchool Report lists specific provisions which should be contained in third-party service provider agreements:

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

[27] We agree with and adopt this approach; third-party service provider agreements must expressly address key access and privacy-related provisions when the arrangement involves personal information. Accordingly, when reviewing such contracts in the context of a privacy complaint investigation, we will expect to see a public body's agreement address: ownership of data; collection, use and disclosure; confidential information; notice of compelled disclosure; subcontracting; security; retention and destruction; audits; and governing law. These expectations reflect fundamental privacy protection principles that are equally necessary under our own legislative framework.

The Department's Contract with PowerSchool

[28] We requested and were provided with a copy of the Department's current contract and agreements with PowerSchool. The current agreement, entered into in 2020, attached and incorporated the terms and conditions found in two prior agreements from 2019, together with an amendment from 2020 (collectively the **"Department's contract**").

[29] Upon review of the Department's contract with Powerschool, we confirm that although several provisions commonly expected in agreements involving the handling of personal information are included, a number of these clauses require strengthening, and additional provisions are needed to address gaps and weaknesses related to privacy protections.

[30] The Department's contract fails to address situations where the service provider may be legally required to disclose personal information, otherwise known as compelled disclosure. This leaves the Department without notice, oversight, or an opportunity to object or limit such disclosure.

[31] The Department's contract also permits the service provider to use and distribute data described as "aggregated and/or de-identified," but does not define these terms or require any standard or methodology for de-identification[15]. While the agreement was amended to restrict the use of such data for targeted advertising or marketing, this does not prohibit disclosure of the purported "aggregated and/or de-identified" data to other entities. Entities may interpret de-identification differently, and if information can reasonably be re-identified, either on its own or when combined with other data, it may still constitute personal information under the Act. Any disclosure of such re-identifiable personal information would constitute an unauthorized disclosure of personal information under the Act. Agreements should avoid reliance on undefined terms such as aggregated, anonymized, or de-identified data, and instead set out clear definitions, standards of de-identification, and restrictions on the resulting data.

[32] The Department's contract appears to have been created by layering multiple agreements, likely carried forward from, or arising out of, the integration of the Newfoundland and Labrador Eastern School District into the Department. This approach has resulted in overlapping and inconsistent provisions. Such agreement layering creates uncertainty about which terms prevail and complicates interpretation, enforcement, and ongoing oversight. It also makes it more difficult for a public body to monitor compliance, as obligations are dispersed across several documents. A more effective practice is to have one agreement with current terms and provisions. Notably absent, and what should have been contained in the Department's contract, is a clear identification of our province's privacy legislation and an explicit requirement for PowerSchool to comply with it.

---

[15] For more information about de-identification see the Ontario Information and Privacy Commissioner's De-identification Guidelines for Structured Data.

[33] The Act requires that the Department put in place reasonable security and information practices to protect personal information. An important step when engaging with a third-party service provider, such as PowerSchool, is to make sure the terms and conditions in the contract expressly require the implementation of reasonable security and information practices to protect personal information. As written, the Department's contract does not adequately reflect or incorporate the terms and conditions necessary for us to conclude that the contract requires the implementation of reasonable security and information management practices.

[34] Notably, the Department's contract has gaps relating to the requirement for PowerSchool to maintain reasonable security measures to protect personal information. The contract references that PowerSchool has a "security program" and "ISO 27001:2013 compliance". However, it does not describe what that security program comprises of, there are no clauses obligating PowerSchool to implement appropriate technical and organizational measures commensurate with the risks associated with processing personal information, nor any detailed articulation of the physical, administrative, technological, or organizational safeguards expected. In addition, the contract does not require compliance with the privacy laws of Newfoundland and Labrador, nor does it specify a requirement for PowerSchool to maintain security measures consistent with industry standards.

[35] It appears that since the Department's contract was originally executed, PowerSchool has developed more fulsome terms as it relates to privacy and security within its updated agreements (see Main Services Agreement and Global Data Privacy Agreement). These current documents contain the types of provisions regarding safeguards, security measures, and compliance expectations that would be expected in agreements where a third-party processes personal information on behalf of a public body. However, the Department's contract does not reference, incorporate, or adopt terms listed in the Global Data Privacy Agreement, or similar terms, nor were we provided with evidence demonstrating that any of those types of terms were added after the Department's contract was formed.

[36] Contractual provisions should ensure that the public body can monitor and verify the third-party's compliance with relevant privacy and security requirements and also require the third-

party to take steps to address compliance issues that are found. As written, the Department's contract does not provide mechanisms through which the Department could compel evidence of compliance. While the Department could nevertheless request such evidence, if PowerSchool were to refuse, there are no clauses obligating PowerSchool to provide it. For example, although the Department's contract refers to the performance of auditing and penetration testing, it does not contractually grant the Department the right to request or receive the resulting reports. The absence of enforceable oversight provisions limits a public body's ability to monitor a third-party's compliance with its contract.

[37] In formulating the recommendations regarding the Department's contract and PowerSchool's security and information practices, we acknowledge using the language articulated in the Ontario IPC's PowerSchool Report.

[38] The Alberta OIPC PowerSchool Report reviewed contract terms that appear to be similar in nature to those set out in PowerSchool's online Global Data Privacy Agreement and Main Services Agreement. The issue was not what PowerSchool stated they would adhere to for privacy protections, but that in reality PowerSchool's practices fell well below the standards set out in its contract.

[39] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend the Department review and, as necessary, renegotiate its agreement with PowerSchool to incorporate or fully address the privacy and security of personal information, including ownership of data, collection, use and disclosure, confidential information, notice of compelled disclosure, subcontracting, security, retention and destruction, audits and governing laws.

[40] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend the Department review and, as necessary, renegotiate its agreement with PowerSchool to include robust contract enforcement provisions to allow the Department to demand documented evidence from PowerSchool demonstrating its compliance with the terms and conditions of the agreement.

[41] **Commissioner's Recommendation:** If it is not possible to review and renegotiate an agreement in a timely manner, pursuant to section 76(2) of the Act, I recommend the Department enter into an addendum to the Department's contract with PowerSchool, until such time as the agreement can be renewed or renegotiated.

[42] The following section outlines specific vulnerabilities and deficiencies identified in PowerSchool's security and information-management practices.

PowerSchool's Security and Information Practices

[43] Powerschool is not a public body subject to our oversight jurisdiction under the Act. The Department, which is a public body subject to our oversight jurisdiction, is fully accountable for the actions of its contractors under the Act. We therefore did not directly investigate the actions of the company PowerSchool unlike some of our counterparts in other jurisdictions. We were able to obtain necessary details about Powerschool's operations primarily through our investigation of the Department, as well as through published reports issued by the Information and Privacy Commissioners of Alberta and Ontario,

[44] In this province, the Privacy Commissioner of Canada, through oversight of the **Personal Information Protection and Electronic Documents Act** (PIPEDA), has jurisdiction over privacy matters involving private corporations such as Powerschool. That Office undertook an investigation of Powerschool which was concluded via a letter of commitment from Powerschool. While Powerschool has therefore been held accountable through other mechanisms, it is essential in this Report that we discuss Powerschool's security and information practices, because as a contractor carrying out work on behalf of the Department, these details are necessary to ensure that we can hold the Department accountable and to make recommendations to the Department for better compliance of the Act when engaging in the future with Powerschool or other such entities.

[45] The Alberta OIPC PowerSchool Report and the Ontario IPC PowerSchool Report provide summaries of their offices' investigations into the security and information practices implemented by PowerSchool. At the time of the cyberattack, PowerSchool had vulnerabilities

and deficiencies in its security and information practices that led to or contributed to the breach. For the purposes of our Office's investigation, we rely on the information provided in both reports to support our recommendations to the Department.

[46] Ontario's Power School Breach Report indicates on page 48 that many vulnerabilities contributed to the threat actor successfully exploiting PowerSchool's education technology, including:

- compromised credentials of a subcontractor with elevated privileges;
- failure to detect four months of unauthorized activities and the cyberattack in a timely manner due in part to limited log retention periods;
- lack of multi-factor authentication required for PowerSource; and
- failure to limit remote maintenance support access on an "as needed basis" only.

[47] Alberta's PowerSchool Breach Report similarly lists deficiencies in PowerSchool's security measures which led to or contributed to the breach at paragraph 176(b):

- failure to adequately identify and address the risks of the remote access for support functions;
- failure to develop, implement and enforce an access control policy that meets industry standards for all levels of administrative level or privileged accounts;
- failure to implement and use multi-factor authentication to access PowerSource and the SISs;
- failure to develop, implement and enforce strong password policies;
- 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;

- failure to identify security vulnerabilities in PowerSource, by failing to classify PowerSource as a critical resource for the purpose of security assessments;
- failure to decommission and securely delete data as required under contractual agreements;
- failure to securely segregate network infrastructures that host PowerSource and SIS; and
- failure to notify Educational Bodies of the Incident in accordance with the terms of agreement with those Bodies.

[48] As identified above, one of the vulnerabilities exploited by the threat actor to exfiltrate data was the "persistent" or "always on" remote maintenance connection; the cyberattack specifically affected instances of PowerSchool SIS where this feature had been enabled, as it allowed continuous remote access through PowerSchool's online support portal, PowerSource. As described in paragraph 65-67 of Ontario PowerSchool Report:

> According to PowerSchool, the institutions could give consent to allow PowerSchool to provide remote maintenance support. If consent was given, it permitted PowerSchool's technical maintenance workers to remotely access the institution's SIS. PowerSchool advised that the default selection for remote maintenance support on either cloud-based or on-premise servers is "off", although the institutions had the option to turn the feature on for a select date range or to select "always on". Further, PowerSchool submitted that the institutions could revoke access for remote maintenance support at any point. In this case, many of the institutions selected the "always on" feature and did not revoke access for remote maintenance support to their respective SIS server. Of note, PowerSchool indicated that those institutions that did not have the "always on" feature on their SIS server were not affected by this cyberattack.
>
> In this cyberattack, the threat actor accessed both cloud-based and on-premise SIS servers in cases where the remote maintenance support feature was set to either "always on" or who had allowed remote maintenance support during the time period when the threat actor had access to PowerSource. I noted that most of the institutions had agreed (consented) to PowerSchool providing such a service as set out in their Agreements, although in some cases the language was not clear.

> Had the institutions disabled or limited access for remote maintenance support on their respective SIS servers to allow access only when the institution required technical support, the magnitude of this cyberattack could have been lessened…

[49] Alberta OIPC's PowerSchool Report questioned whether or not remote access was "enabled by default", as opposed to PowerSchool's position that it was a feature turned on by the education institutions, stating at paragraphs 83-84:

> 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.
>
> 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. 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.

[50] Newfoundland and Labrador's cloud-based instance of PowerSchool SIS also had the "always on" feature enabled, a vulnerability that was exploited by the threat actor and which allowed for the exfiltration of personal information of more than 285,000 individuals from our province's school system. The Department stated that at the time of the incident it was not aware that this feature allowed a persistent connection between PowerSchool SIS and PowerSource. In responding to our inquiry, as to whether this "always on" feature was enabled by default or by the Department, the Department stated it understood that "this feature was enabled early on in the setup of the Department's PowerSchool instance." This "always on" feature has since been disabled from the Department's PowerSchool instance.

[51] **Commissioner's Recommendation:** I recommend the Department limit access to its PowerSchool SIS through PowerSource, or any other remote maintenance support connection, for only as long as necessary to provide the requested technical service.

[52] **Commissioner's Recommendation:** I recommend the Department review PowerSchool's security and information management policies and procedures and associated documentation to ensure they address identified vulnerabilities that contributed to the PowerSchool breach.

[53] PowerSource provided a direct connection to PowerSchool SIS instances, giving access to data containing extensive personal information, yet PowerSource had other significant security vulnerabilities. It relied on single-factor authentication instead of the industry-standard of multifactor authentication, and even its single-factor authentication was inadequate, as its password requirements did not meet industry standards. The Alberta PowerSchool investigation questioned how such vulnerabilities (lack of multifactor authentication, persistent remote connection, etc.) were not identified by PowerSchool.

[54] The standards for what are considered reasonable security arrangements evolve over time in conjunction with changes in the threat landscape. It is not surprising that vulnerabilities can occur. Often entities will conduct periodic assessments using third parties with necessary expertise to identify vulnerabilities which can then be eliminated or mitigated.

[55] In the Department's contract with PowerSchool, signed in 2020, it indicates that security assessment and penetration testing are done on a quarterly basis by an independent third-party:

> As a critical element of our Security Program and ISO 27001:2013 compliance, security assessment and penetration testing are done on a quarterly basis by an independent third-party for our PowerSchool Hosted environment. The security assessment and penetration testing include infrastructure security testing, application security testing, Denial of Service (DoS) testing, and remote access (internal) testing.

[56] What is surprising in this matter is that third-party security assessments and testing did not identify vulnerabilities in PowerSource; the reason why is extremely concerning. Alberta's OIPC PowerSchool Report reviewed the security and penetration evidence provided by PowerSchool, namely the System and Organization Controls ("SOC") 2 Type 2 audit report completed by a third-party for the period of July 1, 2023, to June 30, 2024, and the penetration test report completed by a different third-party for the period of April 30 to June 25, 2024. **Notably, PowerSource was out of scope of both the audit and penetration testing.** The Alberta OIPC PowerSchool Report states at paragraph 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.

[57] Public bodies must implement reasonable oversight measures to make sure service providers are meeting the privacy and security obligations required under the contract.[16] During our investigation, the Department confirmed it was not aware that PowerSource fell outside the scope of PowerSchool's third-party assessments and testing. The Department did provide some evidence[17] that it had reviewed and assessed some aspects of PowerSchool SIS in the past. However, the Department did not provide evidence to show that it monitored PowerSchool's compliance with the security measures set out in the contract.

[58] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend the Department continue to take steps to standardize, define, and document its monitoring of security and auditing provisions under current and future agreements with PowerSchool, and obtain evidence of PowerSchool's fulfillment of its contractual obligations on an annual basis. This includes effective monitoring of PowerSchool's security measures in compliance with

---

[16] Ontario IPC guidance, Privacy and Access in Public Sector Contracting with Third Party Service Providers, at page 3; While the legislation between our provinces differs, the general principles and many considerations listed therein remain relevant.

[17] Review of PowerSchool updates and fixes of known issues, meetings about PowerSchool SIS security measures related to assessment of sensitivity and criticality of information within PowerSchool SIS, technical evaluation.

legal requirements, current industry standards, and best practices that are reasonable in the circumstances.

[59] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend the Department take action to enforce its contractual provisions with PowerSchool, in the event PowerSchool does not comply with its contractual obligations to protect and secure personal information it processes.

[60] Public bodies remain responsible for protecting personal information in their custody and control. When relying on third-party services, public bodies must ensure that an agreement contains contractual provisions that support its compliance with the Act. This includes ensuring the third-party is required to implement reasonable security measures as well as provisions that support a public body's ability to monitor compliance with the agreement. In addition, public bodies must also have reasonable oversight measures in place to monitor a third-party's compliance with the agreement.

[61] The Department's contract with PowerSchool lacked contractual language to demonstrate that reasonable security measures were in place to protect personal information, including the absence of provisions that require PowerSchool to provide evidence of compliance with contractual obligations. The Department did not implement adequate oversight measures to ensure that PowerSchool was adhering to the security measures provided in the agreement or that PowerSchool was implementing reasonable security measures. PowerSchool failed to implement reasonable security measures, and this resulted in a privacy breach for which the Department is accountable.

[62] **Commissioner's Finding:** Given the information before me, I find that the Department did not meet its obligation under section 64(1) of the Act as it relates to the protection of personal information.

Review of Impacted Personal Information

[63] Before reviewing the Department's information practices, it is important to understand the personal information that was impacted by the PowerSchool breach.

[64] The PowerSchool Breach involved teacher and student data from all schools in the province including NLSchools, CSFP, private, and Indigenous schools and impacted **285,158** individuals**.** As part of our investigation we requested a breakdown of both student account input fields (**Appendix B**) and teacher account input fields (**Appendix C**) in our province's instance of PowerSchool SIS. While each type of account has a variety of input fields, only some input fields form a part of the teacher and student table data that was exfiltrated in the breach.

[65] The following table provides a breakdown of the categories of student-related personal information impacted by the PowerSchool breach in our province:

Students*	
Number	• **270,812 Total Impacted** ○ 72,004 with Active Accounts ○ 198,808 with Inactive Accounts / No Longer in K-12
Record Date Range	• **1995 – 2024** • **30 years**
Personal Information (includes all or some combination of)	• Name • Date of Birth • Gender • MCP Numbers • Contact Information • Medical Alert Information • Custodial Alert Information • Discipline Alert Information • Parent/Guardian Contact Information • Emergency Contact Information • Guardian Information • Other Related Information • Social Insurance Numbers (27 instances identified of data that contained 9-digit numbers possibly being a valid SIN)

* In 2020, High School Certification records[18] dating back to 1995 were incorporated into the province's single instance of the PowerSchool SIS. Although we use the term "students," this includes both current and former students. This breach involves both minor children and past students who are now adults.

[66] The Department provided the following descriptions for the categories of student personal information associated with open alert text fields:

- **Medical Alert Information:** This field contains certain medical information provided to a school at the discretion of parents/guardians of a student, including allergy information, medical diagnoses, medical devices, medication information, neurodevelopmental conditions, and mental health conditions.
- **Custodial Alert Information:** This field contains information related to custodial arrangements, including separation or custody arrangements, court orders related to contact/no-contact, emergency protection orders, reference to social worker involvement, as well as other individuals authorized to pick up a student.
- **Discipline Alert Information:** This field contains information related to behavioural or disciplinary matters, such as suspensions, absenteeism, references to behavioural management plan, and behaviour response protocols. These are entered by school administration to note out of the ordinary disciplinary situations that they feel teachers should be aware of (ex. suspension from school).

[67] The following table provides a breakdown of the categories of teacher-related personal information impacted by the PowerSchool breach in our province:

Teacher	
Number	• 14,346 Total Impacted ○ Active Accounts: 7,439 ○ Inactive Accounts: 6,895 ○ Unknown: 12
Record Date Range	• 2010 – 2024 • 15 years
Personal Information	• Name

[18] The Department confirmed the following fields in the High School Certification data were imported into PowerSchool SIS that were impacted by the incident: full name, residential and mailing address, date of birth, gender, MCP number.

(includes all or some combination of)	• Home Address • Personal Email Address • Personal Phone Number • MCP Numbers (60 instances identified) • Social Insurance Numbers (730[19] instances identified) • Date of Birth (1 instance identified; in an inactive account, with name and work email information attached to the DOB)

The Department's Privacy Impact Assessment

[68] Section 72 of the Act requires a public body to conduct a privacy impact assessment in specific and limited circumstances. However, even when a privacy impact assessment is not legislatively required, it remains best practice to complete one for projects involving the handling of personal information, particularly when there is a large amount of personal information or when personal information is highly sensitive in nature. Depending on the nature and sensitivity of the information involved, completing a privacy impact assessment may effectively be a base requirement in order to discharge a public body's obligation under section 64 to take steps that are reasonable in the circumstances to protect the personal information in its custody or control. Conducting a privacy impact assessment helps public bodies identify and mitigate potential risks to personal information within a project. An effective privacy impact assessment details all personal information involved, identifies the legislative provisions that authorize the public body's collection, use, and disclosure of that information, and it identifies risks and mitigation measures.

[69] During our investigation the Department provided us with its **privacy impact assessment** (**PIA**). This PIA was conducted as part of a consolidation project called the Student Administration and Certification System (**SACS**) project which began planning in 2018. PowerSchool's implementation and expansion occurred over many years in our province, starting in 2010 in select public schools and fully expanding to encompass all schools in the province by 2020. PowerSchool SIS was not only expanded to all schools in our province, but

[19] Initial public advisories referred to 749 potential SIN numbers being identified; After further analysis, the Department determined that 19 of those numbers were not valid SINs.

older student records (high school certification records) dating back to 1995 were imported into PowerSchool SIS, as part of a SACS project. A PIA was recommended as part of this project due to the volume of students in the system and the amount of sensitive information contained in the system for each student, the wide range of end users, and the public access needed. The Department confirmed this PIA was begun in May 2018 and completed in January 2021.

[70] Conducting a privacy impact assessment on the information contained within PowerSchool is a reasonable and appropriate information management practice. The Department's PIA includes many of the fundamental elements that our Office expects to see, demonstrating an effort to assess privacy risks associated with the system, however there were some shortcomings.

[71] The PIA did not address the collection, use, or disclosure of **teacher personal information** within PowerSchool SIS. While PowerSchool's teacher accounts included input fields specifically designed for the entry of personal information (home address, email, date of birth), omission of teacher personal information within this PIA or a separate privacy impact assessment represents a notable gap.

[72] The PIA also did not identify the presence of **open text fields** as being a potential privacy risk. Open text fields carry an increased likelihood of containing unnecessary, sensitive, or inappropriate personal information, and as such often require measures to be implemented to minimize these risks (training, reminders, audits, etc). During the investigation, personal information was found in PowerSchool SIS (potential student SIN, teacher SIN, teacher MCP) even though no corresponding text fields existed. The omission of open text field risks in the PIA is a notable gap.

[73] The Department acknowledged that the following information was either collected in error or entered in error, neither of which occurred at the direction of the Department, and has been deleted from PowerSchool SIS:

- student SIN (potential SIN collected in error; no input field existed);
- teacher MCP number (collected in error; no input field existed);

- teacher SIN (entered in error; no input field existed); and
- teacher date of birth (entered in error; input field locked and hidden).

[74] The Department confirmed its decision to remove the following information from PowerSchool SIS:

- teacher home address (removed; input fields locked and hidden);
- teacher personal email (removed; input field locked and hidden); and
- teacher personal phone number (removal ongoing; input field will be locked and hidden).

[75] The Department has confirmed it is conducting a review of open text fields within PowerSchool SIS to assess their necessity and determine whether required fields can be converted to drop-down options. Fields found to be unnecessary are being locked, with existing database entries examined and removed where the information is not required. The Department also confirmed its intentions to update its existing privacy impact assessment which focuses on student information and will also expand the assessment to include teacher personal information stored in PowerSchool SIS.

[76] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend the Department complete a comprehensive review of all open text fields in PowerSchool SIS to confirm their necessity and convert any required fields to standardized drop-down formats to ensure consistency and minimize unnecessary data collection.

[77] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend that all fields identified as non-essential be immediately locked, with the Department reviewing existing entry information and permanently removing any information that is not required for operational or statutory purposes.

[78] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend that the Department update its existing privacy impact assessment on PowerSchool SIS, to reflect

current practices and updates related to student personal information, inclusion of teacher personal information in its assessment, identification of open input fields as a risk and identification of measures being put in place to address this risk.

The Department's Information Management Policies and Practices

[79] We asked the Department whether a retention policy or procedure existed at all as it relates to student personal information. The Department responded by stating a retention policy or procedure did not exist for student personal information in PowerSchool SIS.

[80] The Department explained that a student's record consists of many parts, one of which is the portion contained within PowerSchool SIS and, at the time of the privacy breach, a retention policy or procedure did not exist for student personal information in PowerSchool SIS.

[81] During our investigation the Department provided us with its **Student Record Policy** which addressed both paper and electronic formats of student records. However, at the top of the policy, in red capital letters, is notice from the Department that the policy is under review and destruction of student records is prohibited until further notice. The Department confirmed that this prohibition was implemented in or around October 2024 as the Student Records Policy, as well as all previous NLESD policies, were undergoing a review as a result of NLESD's integration into the Department. The Department also had a concern that the retention period was not long enough[20] for certain records.

[82] The Department explained why the existing policy was applied to paper records only and the need to create a policy to specifically address electronic records contained within PowerSchool SIS:

> When the Student Records Policy was put in place, it was a Policy of the former NLESD. The intention at that time was that the Records Retention and Disposal Schedule referred to in Student Records Policy, while it refers to electronic

[20] The Student Record Policy indicates the minimum period that student records had to maintained (25 years after graduation/school leaving and 15 years for paper school attendance records). It does not specify when any records or portion of records must be destroyed by.

> records, would apply to paper records only, as the necessity at that time was driven by a lack of physical space for record storage. The former NLESD did not have a Records Retention and Disposal Schedule in place specifically for electronic information contained in PowerSchool SIS. In or around 2017, the Department took ownership of PowerSchool SIS. At that time, the Department did not have a Records Retention and Disposal Schedule specifically for electronic files contained in PowerSchool SIS. Given the unique nature of information contained in PowerSchool SIS, the Department is of the view that a specific Records Retention and Disposal Schedule is required.

[83] We also asked the Department whether a retention policy or procedure existed at all as it relates to teacher personal information. The Department responded by stating that no retention policy or procedure exists for teacher information in PowerSchool SIS.

[84] Under the **Management of Information Act**, public bodies are required to put in place a records management system that includes development and implementation of retention and destruction practices. A well-defined retention and destruction schedule allows a public body to securely dispose of personal information that is no longer required and, in doing so, reduces the scope or impact of a potential future privacy breach.

[85] The absence of comprehensive retention and destruction policies and procedures represents a significant governance gap in the Department's information practices. While the Department has a student record policy (under review and with a prohibition on destruction), it did not have in place, nor was it implementing, a comprehensive retention and destruction framework that addressed the personal information stored in PowerSchool SIS for both students and teachers. Establishing and implementing a robust records management system is a reasonable safeguard that public bodies are expected to maintain, as it reduces risks associated with the collection of personal information and helps ensure that only information necessary for operational purposes is retained.

[86] The Department acknowledged that its student record policy review is ongoing, and it intends to apply for approval of a records retention and disposal schedule specific to all information in PowerSchool SIS in accordance with the **Management of Information Act**.

[87] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend the Department develop comprehensive retention and destruction policies and procedures for all student records and teacher records, including records contained within PowerSchool SIS. Once developed, the Department should review the terms of its third-party services agreement and, if applicable, incorporate an ongoing retention and destruction schedule that the service provider must follow during the life of the contract.

Collection of Student MCP Information

[88] During our review of the information categories in PowerSchool SIS, we identified several input fields[21] that appeared to collect information for safety purposes. It was unclear whether the information contained in these safety-related fields was removed once a student exited the K–12 system or if it were maintained for a longer period. The Department confirmed that, apart from student MCP numbers, safety information is or will be removed from PowerSchool SIS:

> With the exception of MCP numbers, student safety information for graduates and former students over the age of 21 has been deleted from PowerSchool SIS. For current students, this is currently being stored in PowerSchool SIS. However, the Department's intention is to have information collected for school safety purposes removed once a student graduates from K-12 or is non-active and over age 21. This will be reflected in the records retention and disposal schedule that is being created for PowerSchool SIS that is being prepared for approval under the Management of Information Act.

[89] The Department confirmed that **244,917 student MCP numbers** were included among the personal information affected by the breach, the majority of which relate to inactive accounts belonging to students who are no longer in the K-12 system (190,651 inactive compared to 54,266 active). As part of the SACs project, student records dating back to 1995 (High School Certification records[22]) were moved into the province's singular instance of PowerSchool SIS

---

[21] Example Input Fields: MCP information, medical alert, special medical considerations, allergies, emergency contacts, parent/guardian alerts, other alerts, etc.

[22] The Department confirmed the following fields in the High School Certification data were imported into PowerSchool SIS that were impacted by the incident: full name, residential and mailing address, date of birth, gender, **MCP number**.

and student MCP numbers from the High School Certification records were included as part of the integration.

[90] This is not the first time the issue of student MCPs has come before our Office. Prior to NLESD's integration into the Department, in Report P-2008-002, our Office investigated a breach involving student personal information and stolen laptop computers. During that investigation we asked NLESD why student MCP information was collected and, at that time, NLESD said it was not in a position to explain how MCP numbers were "necessary for an operating program or activity" of the Department[23]. While the Commissioner at that time did not make a formal recommendation concerning the collection of MCP information, the report did advise that NLESD should stop using MCP numbers for student identification numbers, which was a common practice at that time[24].

[91] With the implementation of the SACs project, the Department was able to move forward with a new method for student identification that would apply across all schools. As confirmed in the Department's PIA, one of the benefits in moving all schools to a singular instance of the PowerSchool SIS was the elimination of using MCPs as student identifiers. Instead, all students, both current and past, were assigned a unique student identification number. Even though student MCP's were no longer needed as a student identifier, they continued to be collected by schools.

[92] In its initial submissions, the Department confirmed that MCP numbers are still being collected and stored in PowerSchool SIS, stating that school administrators use this information in health emergencies and that it is also used to coordinate vaccination programs with public health. When our Office noted the current Information Sharing Agreement with Newfoundland and Labrador Health Services (NLHS) does not list student MCP information, the Department subsequently clarified, that while this information was requested in the past, student MCPs are no longer needed to coordinate vaccination programs with public health.

---

[23] See Report P-2008-002 paragraph 27.
[24] See Report P-2008-002 paragraph 68.

This means that the Department is relying solely on the need to use student MCPs during health emergencies as its basis for collecting this information.

[93] In discussions with NLHS, it was confirmed that individuals will not be denied access to medical services within the provincial healthcare system in the event of a medical emergency, even if they do not have, or are unable to present, an MCP card or number. Emergency medical services are available to all individuals in need, regardless of whether they possess or provide MCP information. We indicated to the Department that based on this information, the collection of student MCP information did not appear to be necessary for students to receive emergency medical services.

[94] We asked the Department if there was any additional information it would like us to consider given that student MCP information did not appear to be necessary for the purposes identified as the reason for its collection by the Department. The Department responded with the following information:

> The collection and use of MCP numbers for this purpose was an ongoing past practice. School administrators reported that in the past first responders requested MCP numbers when they arrived at schools to attend medical emergencies. Administrators were told by past health services staff to keep MCP numbers in case of emergencies. In light of recent discussions with officials from HCS and NLHS in the past year, it was determined that the collection of student MCP numbers may no longer be needed.

[95] The Department also identified that student MCP information contained in PowerSchool SIS would be highly beneficial to a number of NLHS public health activities, as well as a research project, which could be used with other information in PowerSchool SIS and the health care system. The Department indicated wanting additional time to determine the extent and form of the information that could be disclosed for these purposes, and indicated its intentions to maintain the collection of student MCP numbers.

[96] While information contained in the PowerSchool SIS, including student MCP numbers, may be requested by or useful to other entities if disclosed, this does not, on its own, establish a lawful purpose for the Department's collection of MCP information. Under the Act, a public

body must have clear and explicit authority to collect personal information before it can consider any subsequent use or disclosure. Without this collection authority, neither the use nor disclosure of MCP numbers can be justified.

[97] The Department's Student Record Policy does not specifically address student MCP numbers but does refer to a student's cumulative file containing "medical information necessary to be easily accessed in an emergency situation" and lists as an example "procedure to follow if child is anaphylactic or diabetic". The policy does speak to collection of student information, stating that:

> Student information is collected, and student records are established for the general purposes of providing instruction to students; ensuring the delivery of educational programming and services and the safe, orderly functioning of the school, and documenting decisions made about the education of a student.

[98] The Department's PIA did address "Student MCP", describing it as "Students MCP number and related expiry date", and listing its reason for collection as "Needed for medical emergencies at schools should student require immediate medical attention". The PIA also specifies the purported legislative authority for collection of this information stating:

> Section 12(1) of the Schools Act states "A student records shall be maintained for each student in the manner required by a policy directive of the minister." Section 12 also states that the student record may be used to assist in the instruction of the student (12(5)); to prepare information as required by the Schools Act, to an Educational Institution or an application of employment (12(7)), and for diciplinary (sic) proceedings (12(8)).
>
> The Department currently does not have a policy directive in place. The need for a policy directive has been identified. When developed, the policy will better define the student record and the roles and responsibilities of the department and schools.
>
> When the policy directive is in place, the authority for collection will be under section 61(a) of ATIPPA, 2015 and section 12 of the Schools Act. Until the policy directive is in place, section 61(c) of ATIPPA may be cited provided that the information relates directly to an [sic] is necessary for an operating program or activity of the schools.

[99] Section 61(a) of the Act states that "No personal information may be collected by or for a public body unless the collection of that information is expressly authorized by or under an

Act". For the legal authority to come from section 61(a), the collection must be "expressly authorized" either by an act (collection is specified in the act) or under an act (the act specifies that collection of personal information is permitted under another instrument).

[100] Regarding "by an act", the **Schools Act, 1997** does not expressly authorize the collection of MCP information by the Department or by any other schools. Regarding, "under an act", while a policy directive is a type of instrument that could fall into this category, the policy directive referred to in section 12(1) of the **Schools Act, 1997**, authorizes the minister to give directives about record maintenance:

> 12(1) A student record shall be maintained for each student in the manner required by a policy directive of the minister.

Under section 12(1), the minister is being given the authority to provide instructions on how an existing record (information that is already collected) is to be maintained; this section does not expressly authorize the minister to make a policy directive on the collection of student personal information.

[101] Based upon the information provided to our Office, the Department cannot rely on section 61(a) of the Act as authority for its collection of student MCP information as the Department's collection of student MCP information is not expressly authorized by or under an act.

[102] The Department's PIA also listed section 61(c) of the Act as legal authority for collection of student MCP information, which states that "No personal information may be collected by or for a public body unless that information relates directly to and is necessary for an operating program or activity of the public body."

[103] The Department's PIA indicates that student MCP numbers are collected and used by school administrators to respond to health emergencies. The Department's submissions further confirm that collecting MCP numbers for this purpose was part of an ongoing practice, as school administrators were routinely asked to provide MCP numbers when first responders attended the school for emergency situations.

[104] It does not appear, nor did we receive any evidence, indicating the Department or its predecessors asked for information as to why first responders were requesting that information. As indicated above, NLHS has confirmed to our Office that individuals will receive emergency medical services even if they do not have, or are unable to present, an MCP card or number. The fact that student MCP numbers may be sought by other individuals or entities does not, on its own, justify or legally authorize the Department's collection of this information.

[105] Based upon the information provided to our Office, the Department has not demonstrated that student MCP information is needed by the Department for its delivery of educational programming and services and therefore collection of student MCP information is not authorized under section 61(c).

[106] **Commissioner's Findings:** Pursuant to section 76(2) of the Act, I find the Department has not demonstrated that it has the legal authority under the Act to collect student MCP information. I find this is an overcollection of student personal information, which has resulted in an increased risk of harm to individuals impacted by the privacy breach.

[107] We note that other Canadian jurisdictions have come to similar conclusions. In the Ontario IPC PowerSchool Report[25], many schools acknowledged that they were not authorized to collect student health care numbers and the Ontario Commissioner recommended they stop collecting student health card numbers as collection of this information was not necessary to fulfill their educational mandate. In the Saskatchewan OIPC PowerSchool Report[26], the Saskatchewan Commissioner stated there is no need for a school to collect a student's health services number, and this overcollection aggravated the extent of the exfiltration of personal information in the privacy breach. The Saskatchewan Commissioner recommended the school stop collecting student health services numbers and to purge this information from any past

[25] See MR25-00002 et al at paragraphs 163 and 169; For the purposes of this paragraph, "schools" refers to the Ontario school boards, which, along with the Ministry of Education, are described as "institutions" in the Ontario IPC PowerSchool Report.
[26] See 003-2025, 035-2025 at paragraphs 32 and 71; For the purposes of this paragraph, "school" refers to the named school division in the Saskatchewan PowerSchool Report.

and present student records held by the school or by its current information management service provider.

[108] If the Department wishes to have the authority to collect student MCP information, legislative amendments are required to expressly permit such collection. Any proposed changes would then proceed through the legislative process, allowing for public debate and ensuring transparency regarding the scope and implications of this new authority.

[109] **Commissioner's recommendation:** Pursuant to section 76(1)(a) of the Act, I recommend the Department stop collecting, using, or disclosing student MCP information.

[110] **Commissioner's recommendation:** Pursuant to section 76(1)(b) of the Act, I recommend the Department destroy and purge student MCP information from all student records[27], including but not limited to, destruction and purging of this information from PowerSchool SIS, electronic records, and paper records.

ISSUE #2: RESPONSE TO THE PRIVACY BREACH

[111] The Access to Information and Protection of Privacy (ATIPP) Office has developed a Privacy Breach Protocol to support public bodies in responding to a privacy breach. The protocol provides a practical framework for managing a breach, outlining key steps such as containment, risk assessment, notification, and prevention.

Containment

[112] The purpose of containment is to minimize (stop or reduce) the risk or damage caused by the privacy breach. During this step, some investigation efforts take place. Information gathered through investigation of the breach assists public bodies in making decisions on

[27] The Department describes the official repository of student records as a combination of: "(1) PowerSchool SIS, Review 360, and Responsive Teaching and Learning database electronic records; and (2) paper files stored in schools or an alternate location (active student files are maintained at the school the student is currently attending. Students who have graduated may have their file stored in an alternate location)", noting that every student would have a cumulative file and some students would also have a confidential file.

what containment measures to take and how to implement them. Effective and prompt containment may reduce the magnitude of a breach, and may, in some cases, reduce the risks to individuals impacted by the breach.

[113] On December 28, 2024, PowerSchool became aware of the incident. Upon discovery, PowerSchool initiated its cyber security incident response protocol and organized a cross-functional response team, including third-party cyber security experts, to contain the threat and determine the scope of the cyberattack[28]. CrowdStrike, the third-party cyber security firm retained by PowerSchool, conducted the investigation, and its methods and investigation findings are summarized in the Crowdstrike Investigation Report.

[114] As mentioned earlier in this Report, upon receiving notification from PowerSchool on January 7, 2025, the Government of Newfoundland and Labrador (GNL) initiated its own incident response for cyber and privacy investigations. Part of the investigation steps taken included GNL contracting with a cyber security service provider to validate the forensic information provided by PowerSchool and CrowdStrike. The decision to retain independent third-party experts to verify PowerSchool's investigative findings constituted a prudent and reasonable approach to ensuring a thorough and reliable examination of the breach. The service provider was able to verify investigatory findings, and confirmed the threat actor gained access to GNL's PowerSchool SIS data between December 20-22, 2024.

[115] The primary containment actions during this breach were undertaken by PowerSchool. As outlined in the Crowdstrike Investigation Report, upon being made aware of the cyberattack PowerSchool indicated it took the following containment steps:

- Deactivating the compromised credential;
- Enforcing a full password reset for employees and contractors;
- Restricting access to and tightening password and access controls for the affected customer support portal; and

[28] MR25-00002 et al at paragraph 16.

- Requiring that access to the PowerSource environment be via company's VPN, which requires single sign-on (SSO) and multi-factor authentication (MFA).

[116] The Ontario IPC PowerSchool Report commented on PowerSchool's containment efforts stating at paragraphs 173-174:

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

[117] Once personal information has been exfiltrated, a breach can never be fully contained because it is impossible to determine with certainty what a threat actor does with the data thereafter. Even when a ransom is paid on the basis of assurances that information will be deleted, those assurances cannot be verified. As stated in our Report[29] outlining the investigation into the 2021 cyberattack on the province's healthcare system:

> Insofar as containment efforts are concerned, payment or nonpayment of ransomware results in the same conclusion: the privacy breach not being contained. Payment of ransom cannot be relied upon as an effective containment solution as there is no way to confirm stolen data was wholly deleted and not retained. Similarly, non-payment of a ransom cannot be said to be a "bad" containment decision since payment does not necessarily equate to effective containment.

[118] In this case, PowerSchool paid a ransom after receiving promises that the exfiltrated information had been deleted. However, the same data was used in an attempt to extort PowerSchool's clients directly, including schools within Canada. While the Department did not find evidence of any direct extortion attempts involving schools in this province, the personal information of 285,158 individuals involved in the school system in Newfoundland and Labrador was taken, and the breach was not fully contained.

---

[29] See Report P-2023-001/PH-2023-002 at paragraph 119.

[119] **Commissioner's Finding:** I find that the personal information exfiltrated in this matter was not contained. However, I find that reasonable steps were taken to contain the breach to the extent possible.

[120] We do wish to note that the enrollment deadline for the two-year credit-monitoring and identity-protection services previously offered to impacted individuals is now expired. Individuals who now become aware that their information was impacted will no longer be able to avail of these services. In the cyberattack against the province's health care system, NL Health Services not only offered credit monitoring services to affected individuals, but also implemented its own dark web monitoring to support ongoing efforts to detect, respond to, and mitigate potential misuse of compromised information[30]. In the PowerSchool breach there exists evidence of misuse, as at least some of the data taken was not deleted, and in other jurisdictions was used in additional extortion attempts. Given these circumstances, we strongly encourage the Department to consider implementing similar dark web monitoring measures to enhance its response and ongoing mitigation efforts.

Evaluation of the Risks

[121] Assessing the potential risks to affected individuals is essential to understanding the scope of the breach and the ways in which it may impact those whose personal information was compromised. As stated in prior reports[31] of this Office:

> This evaluation assists in determining whether notification is necessary, and if so, how it should be done and what information it should contain. The more sensitive the information, the importance of notification increases and the manner in which it is done becomes more important. Once those individuals whose personal information is involved in the breach are aware of the breach and what information was potentially or actually exposed, they, along with the public body, can take appropriate steps to mitigate any potential risks associated with the information being disclosed.
>
> ...
>
> Further considerations in evaluating the risk include determining the cause and extent of the breach, which can indicate whether the information was lost or stolen, or whether the breach was deliberate or accidental, whether the

[30] Report P-2023-001-PH-2023-002.pdf at paragraph 105.
[31] See Reports: P-2008-003 at paragraph 8; P-2009-001 at paragraph 7; P-2008-001 at paragraph 20; P-2023-001-PH-2023-002 at paragraph 125.

> information can be recovered, or whether the breach was due to a systemic problem or an isolated incident. The process of evaluating the risk also includes identifying who and how many people may have been affected by the breach, as well as assessing the foreseeable harm which might come from the breach.

[122] The type of information taken in this breach is explained in depth elsewhere in this Report. In general, it includes a variety of information types, including SINs, MCP numbers, date of birth, gender, contact information, medical information, custodial information, disciplinary matters, etc. While many adults were affected by this breach, including current and former teachers as well as former students who are now adults, a significant portion of the compromised information relates to minor children, who are recognized as a particularly vulnerable group. The type of information accessed and stolen in this attack can be used for fraudulent and other harmful purposes.

[123] This breach was caused by the malicious actions of a threat actor trying to extort payment. The likelihood of harm is increased as there can be no certainty that the information taken in the PowerSchool breach will not be misused at some point in the future.

[124] The foreseeable harm from a privacy breach is not limited to the impacted individuals, there exists a risk of harm to public trust. This incident represents the second largest breach of personal information ever experienced in the province. The first was the cyberattack on the provincial healthcare system, which affected nearly every resident of Newfoundland and Labrador. Now, with the PowerSchool breach, the province's education system was impacted. Together, these breaches risk eroding public confidence in the ability of public institutions to safeguard the personal information entrusted to them.

[125] **Commissioner's Finding:** I find that the personal information taken by the threat actor includes highly sensitive information.

[126] **Commissioner's Finding:** I find that there is foreseeable harm to individuals impacted by the privacy breach as a result of this information being compromised due to malicious actions and the inability to fully contain exfiltrated data.

[127] **Commissioner's Finding:** I find that there is a risk of significant harm within the meaning of section 64(8) of ATIPPA, 2015.

[128] The Department undertook several steps that demonstrate meaningful efforts to assess the risks arising from the breach and to take timely action in response. Immediately after becoming aware of the incident, the Department moved to ensure that known information was communicated to the public, issuing public advisories, providing information online, disseminating information to schools, to our Office, and the Newfoundland and Labrador Teachers' Association, reflecting an early recognition of the need to manage potential harms.

[129] The Department also undertook a targeted risk-assessment process to identify individuals who required additional notification following the PowerSchool breach. To do so, it first reviewed the student and teacher tables within PowerSchool SIS to understand the types of information stored and the number of individuals affected. It then used keyword searches to locate potentially sensitive information and identified six open text fields requiring closer examination. These fields were manually reviewed and categorized by sensitivity, after which the results were matched to individual students to determine how many active students had higher-risk information. The Department provided direct notification to teachers due to the sensitivity of the SIN information being impacted by the breach, which was sent out between January 31 – February 7, 2025 via email or registered mail. The Department issued additional direct notifications to the parents or guardians of those students whose personal information was assessed by the Department as higher risk, with these notifications being sent on July 25, 2025. These actions indicate that the department continued to assess the nature of the breach and make additional notification efforts associated with heightened risk and we commend them for taking these additional steps related to highly sensitive personal information.

[130] The early actions taken demonstrate that the Department began assessing the nature and scope of the breach at an early stage. The Department's subsequent decision to issue direct notification letters to individuals whose information it identified as higher sensitivity further indicates that it continued to evaluate risk throughout its response. While these efforts reflect

a reasonable approach to risk assessment, notification is a distinct issue and will be addressed separately in the following section.

[131] **Commissioner's Finding:** I find that the Department took reasonable steps to evaluate the risks in response to the PowerSchool breach.

Notification

[132] Pursuant to section 64(3) of the Act, our Office is required to be notified of a breach of personal information in the custody or control of a public body. Depending on the nature of the privacy breach, it may also be appropriate for public bodies to contact law enforcement and other professional or regulatory bodies. While notification requirements to other entities are not specifically outlined in the Act, we do consider such notifications when assessing whether reasonable steps were taken in responding to a privacy breach.

[133] On January 7, 2025, the Department was given notice by PowerSchool that a cyber security incident had occurred impacting some PowerSchool SIS instances.

[134] On January 8, 2025, the Department contacted our Office to report the incident and, by the end of the day, submitted its privacy breach report in compliance with section 64(4) of the Act. That same day, the Department also notified the CSFP, private schools, Indigenous schools, and the Newfoundland and Labrador Teachers' Association ("**NLTA**"). In addition, the Department issued a memo to NLSchools parents and guardians and a public advisory confirming information known at the time. The Minister of the Department also held a media availability.

[135] At that stage, the only confirmed information was that PowerSchool had experienced a cyber security incident, that its platform is used throughout the province's K–12 education system, and that work was underway in our province to determine the extent of the data accessed and the number of individuals potentially affected. The Department acted promptly by engaging with partner organizations, the public, and the media, sharing the information available at the time, and formally reporting the breach to our Office.

[136] **Commissioner's Finding:** I find that the Department's efforts to share the general information available to it about a large-scale breach impacting the province's K–12 education system constitutes a reasonable and appropriate response to the initial stages of managing a large-scale privacy breach.

[137] Under sections 64(3) and 64(7) of the Act, public bodies are required to notify individuals whose personal information is stolen or accessed by an unauthorized person, if the privacy breach creates a risk of significant harm to the impacted individual. Section 64(8) of the Act indicates that "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. Under section 64(9) of the Act, two factors relevant to determining the risk of significant harm, include, but are not limited to the "sensitivity of the personal information" and the "probability that the personal information has been, is being, or will be misused".

[138] As noted earlier in this Report, the data that was unlawfully accessed and taken in this breach includes highly sensitive personal information that carries a high risk of misuse by malicious actors and, consequently, an increased risk to impacted individuals. There is a foreseeable likelihood of harm resulting from the compromise of this information, given both the malicious nature of the threat actor's actions and the inability to fully contain the exfiltrated data.

[139] **Commissioner's Finding:** I find that the factors in this matter establish a risk of significant harm to impacted individuals within the meaning of the Act, and accordingly, the Department is obligated to notify those individuals under section 64(3).

[140] Decisions about how to notify individuals impacted by a privacy breach require an assessment of the particular circumstances of each case, with mitigation of harm being a key consideration. In most circumstances, reasonable notification will require direct notification[32]

[32] Examples of direct notification include: telephone, mail, email, virtual meeting, in-person decision

to affected individuals. Indirect notification[33] may be used when providing direct notice is not reasonably practical or feasible. Where direct notification does not occur, our Office will take into consideration many factors, including whether direct notification would cause undue hardship to the public body, and whether there are substantial and compounding issues associated with practicality or accuracy of older contact information, risks of further privacy breaches, etc.

[141] In some situations, using multiple notification methods may serve as an effective approach for notifying impacted individuals. However, public bodies should be careful when using this approach to make sure information remains consistent and notification details are clear.

[142] While initial general information was provided on January 8, 2025, once further details about the breach became available, the Department implemented multiple notification methods, which are summarized below:

- **January 28, 2025 Indirect Notifications:** a Public Advisory was issued by the Department in a News Release and a memo was sent to staff and families from NLSchools identifying categories of impacted individuals and confirming that GNL is working with PowerSchool on notification processes;
- **January 31 - February 7, 2025 Direct Notification:** Teachers whose personal information taken in the breach also included their SIN information were sent a direct notification letter (email or mail) from NLSchools;
- **February 4, 2025 Indirect Notification:** a Public Advisory was issued by the Department in a News Release confirming credit monitoring and identity protection services are now available to those impacted, noting PowerSchool (through Experian) will also be sending direct email notifications to those individuals for whom they have sufficient contact information;

[33] Example of indirect notification include: written public advisory/news release, and in person or electronic public advisory briefing, news releases, website notifications, social media postings, newspaper advertisements.

- **February 20, 2025 Direct Notification:** Email from PowerSchool sent to students and educators, confirming the name of the impacted person, types of personal information exfiltrated in the breach, and information about enrollment in credit monitoring and identity protection services;
- **February 21, 2025 Indirect Notification:** a Public Advisory was issued by the Department in a News Release confirming what email addresses were used to send PowerSchool's notification, and warning individuals to check their spam/junk email folders as this was an official email from PowerSchool;
- **July 25, 2025 Direct Notification:** Students with an active status, whose personal information taken in the breach also included information assessed by the Department as higher risk, were sent direct notification letters (emails) from NLSchools to the student's parent or guardian; and
- **Various Dates Indirect Notification:** The Department published information on its website, including its public advisories, links to PowerSchool's website regarding the breach, and additional details in a frequently asked questions section.

[143] While our investigation focused on the Department's own notification efforts, we did ask the Department to confirm the number of individuals who did or did not receive PowerSchool's direct notification email. The Department explained that some of its staff did not receive the notification despite being among those who should have, but it could not provide any additional information about who did or did not receive PowerSchool's February 20, 2025 notification.

[144] The Department primarily relied upon indirect notification methods to inform individuals affected by the PowerSchool breach. Direct notification was provided to a small subset of affected individuals where reliable contact information was available, and a higher level of risk had been identified by the Department. Decisions regarding direct notification were based on the Department's risk assessment and the

availability of reliable contact information, resulting in direct notification for the following groups:

- **~5% of teachers**, namely 363 active and 367 inactive, who had their **SIN information** taken in the breach; and
- **less than 2% of current students** (active) who had personal information the Department assessed as **higher risk** taken in the breach.[34]

[145] Outdated contact information increases the risk of additional privacy breaches, with the level of risk increasing as the information becomes older. In this case, contact information associated with former teachers dated back as far as 15 years, while student records were dated back 30 years. Although the Department maintains up-to-date contact information for currently enrolled students and active teachers, the number of individuals impacted by the breach remained substantial. Given the scope, context, and circumstances of the breach, issuing direct notification letters to each affected individual was not reasonably practical or feasible.

[146] **Commissioner's Finding:** I find that the Department's decision to rely primarily on indirect notification methods to inform the majority of individuals affected by the PowerSchool breach was reasonable in the circumstances and an appropriate response to managing a large-scale privacy breach.

[147] **Commissioner's Finding:** I find that the Department's use of a risk-based assessment to determine and issue a limited number of direct notifications was a reasonable approach and an appropriate response to managing a large-scale privacy breach.

---

[34] The Department initially flagged 1,237 active student accounts as potentially containing highly sensitive information. After completing a manual review of these accounts, the Department (NLSchools) sent direct notification emails to the parents or guardians of those students whose information was assessed as being higher risk. This means that fewer than 1% of current students received direct notification from the Department, which represents less than 0.4% of all past and current students who were impacted by the breach.

[148] Absent from the Department's direct notification efforts were the student records that had potential SIN information taken. The Department's analysis of student data identified 27 instances of 9-digit numbers that could be a valid social insurance number. The Department explained that its classification of the numbers as being "potential" SIN, is because it does not retain any SIN information for students that would allow it to validate this information. In outlining its reasons for not directly notifying these individuals, the Department explained:

> The Department also wishes to note that it contacted numerous school administrators who advised that teachers or other school staff did not collect social insurance numbers for students.
>
> However, with regard to the 27 instances of possible social insurance numbers, only 14 of those students are currently enrolled students. The Department would not send any direct notifications to unenrolled students out of concern for the potential of a secondary privacy breach, given that the address information for students that are no longer enrolled may not be current and that these students may be over the age of 19.
>
> With regard to the 14 students currently enrolled, none of these students had other information in PowerSchool SIS that was determined to be in the high risk category. As a result, given that these numbers are only potential social insurance numbers, and given the public notifications previously made by the Department referred to in the Department's earlier answers, the Department determined that further direct notifications were not necessary.

[149] As indicated above, the Department's reliance on indirect notification methods for individuals with dated contact information, which includes former students[35], was appropriate and reasonable in the circumstances given the additional privacy risks associated with dated contact information. However, current students are required to update their contact information annually, which makes the likelihood of outdated information low. Although the Department has described this as "potential" SIN information, it has not provided any evidence clarifying what the 9-digit numbers actually were. Given that these individuals are current students, the high sensitivity and risk associated with SIN information, and the fact that the information was taken by a malicious threat actor, the risk of harm is significant and direct notification is warranted.

---

[35] The **former students** being referred to in this paragraph and elsewhere in this Report refers to the 198,808 individuals who are no longer in the K–12 education system. Given that the dataset includes students enrolled since 1995, approximately 30 years ago, the majority of these individuals are now adults.

[150] **Commissioner's Finding:** I find the Department's reliance on indirect notification methods for current students whose personal information included potential SIN information to be unreasonable.

[151] **Commissioner's Recommendation:** I recommend that the Department provide direct notification to the parents or guardians of the 14 currently enrolled students whose potential SIN information was taken in the breach.

[152] While the Department's notification methods were largely reasonable and appropriate, we did identify areas where the clarity of the Department's breach communications could be improved.

[153] In our review of the Department's indirect notifications, the wording used throughout does not make it clear that the large majority of individuals impacted by this breach would not be receiving direct notification letters.

[154] While the Department's January 28, 2025 public advisory referred to impacted groups, it also indicated that GNL was "working with PowerSchool on notification processes…". Further public advisories focused on providing other information, including status updates on notifications. The February 4, 2025 public advisory indicated that "direct email notifications" would be sent out from PowerSchool (for those affected individuals for whom they have sufficient contact information); the February 21, 2025 public advisory references Powerschool sending an email to "those affected". The Department's public advisories give the impression that affected groups would receive direct notification from either the Department or PowerSchool. This perception is reinforced on the Department's webpage, which states in its FAQ section:

> **How do I know if my data was accessed?**
> In the coming weeks, Experian (on behalf of PowerSchool) will be distributing direct email notifications to involved students (or the parents/guardians of students, as applicable) and educators for whom they have sufficient contact information. The email notice will include further information about the information of theirs involved and the resources PowerSchool is offering.

> The Department of Education will provide individual notifications to the 749 individual teachers who had a SIN involved in the breach.

[155] The Department's indirect notifications failed to explicitly acknowledge that it would be unable to provide direct notification to all impacted individuals. Consequently, the messaging lacked clarity and risked giving individuals a false sense of reassurance, potentially leading them to conclude that "no news is good news."

[156] **Commissioner's Finding:** I find the Department's indirect notifications lacked the clarity needed to prevent misunderstanding, resulting in a significant gap in its breach response.

[157] Our Office recommends several best practices to address this potential issue. When a public body uses multiple notification methods and intends to directly notify only some of the individuals affected by a breach, this limitation should be stated clearly in any indirect notification. If the analysis is still underway and it remains uncertain whether direct notification to all impacted individuals will be possible, that uncertainty should also be explicitly communicated. In situations where it is known in advance that not everyone can be contacted directly, the indirect notification should clearly advise that some affected individuals will not receive direct notice and should include an explanation of why universal direct notification is not feasible. Any subsequent updates related to notification should continue to reiterate this information to ensure clarity.

[158] Providing this clarification promotes transparency and helps mitigate confusion, especially in large-scale breaches where direct notification is feasible for some, but not all, affected individuals. While it may not eliminate confusion entirely, clearly communicating these limitations reduces the risk that individuals will wrongly assume they were unaffected solely because they did not receive a direct notification letter.

[159] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend the Department clearly communicate in all of its future indirect notifications and subsequent notification updates, whether direct notification will be provided to all impacted individuals and, if not, the reasons why.

[160] The Department's webpage about the PowerSchool Breach requires significant updates to reflect accurate and current information. While its webpage provides a chronological list of advisory notices, the Frequently Asked Questions (FAQ) section, which should serve as the most visible and up-to-date source of consolidated information, is notably inaccurate and out of date. These inaccuracies include, but are not limited to: the FAQ section continues to reference credit monitoring and identity-protection services that are no longer available for enrollment; it repeats PowerSchool's earlier "belief" that the compromised data had been deleted, even though subsequent evidence indicates the data had not been deleted and was later used in a second extortion attempt; and it potentially provides readers with the false impression that direct notification letters were sent to all individuals impacted by the breach. Failure to maintain this webpage represents a demonstrable gap in the Department's response to the breach.

[161] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend the Department update its webpage to ensure accurate and accessible information, and I recommend that the Department clearly communicate in its FAQ section that not all impacted individuals will receive direct notification, and explain the reasons why.

Prevention

[162] Prevention is a critical component of managing a privacy breach. It is essential for a public body to conduct a thorough investigation to understand what occurred, identify root causes, and assess the factors that contributed to the breach. This analysis is key to reducing both the likelihood of a future incident and the severity of harm should one occur. The ultimate objective is to ensure that all risks identified through the investigation are addressed to the fullest extent possible, thereby meaningfully mitigating the potential impact of any future breach.

[163] There were significant gaps and vulnerabilities in PowerSchool's security measures and practices that caused or contributed to the breach, enabling the threat actor to successfully exploit PowerSchool's education technology and exfiltrate the personal information of 285,158 individuals associated with the school system in this province. The Ontario OIPC

PowerSchool Report[36] outlines some of the remedial measures that PowerSchool implemented after the breach:

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

[36] See MR25-00002 et al at paragraph 202.

- configuring its systems and data storage with AES-256 encryption for data at rest.

[164] On July 15, 2025 PowerSchool signed a Letter of Commitment, with the Federal Privacy Commissioner's Office, in which it agreed to a series of remedial and preventative measures, some of which should already have been completed and others that are scheduled for implementation in the near future, including the following:

- By July 31, 2025, PowerSchool will confirm to the Commissioner whether it has contracted and/or will receive any additional forensic information or recommendation(s) about the incident from CrowdStrike or other forensic investigative entities other than those already included in the March 2025 report, and if so, will provide a copy of the information;
- By July 31, 2025, PowerSchool will confirm to the Commissioner whether it plans to implement any additional authentication process for the PowerSource platform and provide details explaining the additional measures including dates of implementation. Should PowerSchool choose to not implement an additional authentication process, it will provide to the Commissioner a detailed explanation;
- By December 31, 2025, PowerSchool will provide the Commissioner evidence that will clearly demonstrate that 1) it has strengthened its monitoring and detection tools and 2) its tools can identify patterns of irregular activity;
- By December 31, 2025, PowerSchool will provide the Commissioner evidence that will clearly demonstrate that it has conducted a review and readjustment of its system access privileges to align with security best practices and operational needs, including customer support agents;
- By March 31, 2026, PowerSchool will provide the Commissioner with information demonstrating that it has obtained recertification of ISO/IEC 27001 compliance;

- By March 31, 2026, PowerSchool will provide the Commissioner with a security assessment and report conducted by an accredited and independent external security assessment firm that assesses PowerSchool's updated information security safeguards, which will include at a minimum:
    - an assessment of the effectiveness of PowerSchool's safeguards to protect personal information;
    - an assessment of PowerSchool's ability to prevent, detect, and respond to potential breaches;
    - the identification of any internal and external risks that could potentially affect personal information; and
    - solutions to address those risks.
- If the security assessment firm issues recommendations to PowerSchool in the context of the assessment, PowerSchool will provide a copy of the recommendations and inform the Commissioner of the following:
    - whether PowerSchool has accepted each of the recommendations;
    - if not, the reason why; and
    - if accepted, whether the recommendation has been fully implemented and actions taken by PowerSchool to implement the recommendation, and if not yet fully implemented, PowerSchool will provide to the Commissioner an implementation plan, detailing the actions PowerSchool will take to implement the recommendations and dates by which these actions will be completed. The recommendations (or lack thereof) and their implementation will be subject to review and approval by the Commissioner.

[165] **Commissioner's Recommendation:** Pursuant to section 76(2) of the Act, I recommend the Department follow up with PowerSchool to request information and evidence of actions PowerSchool committed to undertake as part of its Letter of Commitment with the Federal Privacy Commissioner's Office.

[166] The Department relies on the Letter of Commitment to confirm the prevention measures taken by PowerSchool and we are recommending the Department follow up directly with PowerSchool to ensure its commitments are completed. However, as outlined earlier in this Report, the Department's contract does not contain provisions that would allow it to compel evidence of compliance, nor does it provide mechanisms for the Department to monitor and verify PowerSchool's adherence to relevant privacy and security requirements. The lack of oversight provisions, along with the additional gaps and vulnerabilities previously identified, form the basis of several recommendations we have made to the Department to strengthen its agreement with PowerSchool. Until these agreement issues are addressed, the current terms of the Department's contract remain a source of ongoing risk that has not been fully mitigated.

[167] In addition to the measures outlined by PowerSchool in the Letter of Commitment, the Department confirmed, with the assistance of the OCIO, the implementation of several mitigation measures that focus on enhancing identity lifecycle management (ILM), authentication, authorization, and data management. The Department also deleted unnecessary information from PowerSchool SIS and, where appropriate, locked and hid the related input fields to prevent further overcollection and reduce impact risk. The Department is reviewing all open text fields in PowerSchool SIS and will adjust field configuration to further reduce impact risk. The Department has also committed to updating its existing privacy impact assessment on personal information stored in PowerSchool SIS. These prevention measures demonstrate reasonable steps towards mitigating the risk and potential impact of a future breach involving PowerSchool SIS.

[168] Implementing a robust, comprehensive records management system is a reasonable safeguard that public bodies are expected to maintain. Such a framework reduces the risks associated with retaining unnecessary personal information and minimizes the impact of any future privacy breach. While the Department is taking reasonable steps towards addressing this governance gap by addressing personal information stored within PowerSchool SIS, the lack of comprehensive retention and destruction policies and procedures that apply to all of the Department's student and teacher records represents an ongoing risk that has not been fully mitigated.

[169] With respect to student MCP information, the Department acknowledges that "the collection of student MCP numbers may no longer be needed", but that it plans to continue collecting the information from students. Earlier in this Report, we have recommended that the Department stop collecting student MCP numbers and delete and purge existing MCP information from its records. Until these steps are completed, the continued collection and retention of student MCP information represents an ongoing risk that has not been fully addressed by the Department.

SUMMARY OF COMMISSIONER RECOMMENDATIONS

[170] The following is a summary of all commissioner recommendations made in this Report:

i. Pursuant to section 76(2) of the Act, I recommend the Department review and, as necessary, renegotiate its agreement with PowerSchool to incorporate or fully address the privacy and security of personal information, including ownership of data, collection, use and disclosure, confidential information, notice of compelled disclosure, subcontracting, security, retention and destruction, audits and governing laws.

ii. Pursuant to section 76(2) of the Act, I recommend the Department review and, as necessary, renegotiate its agreement with PowerSchool to include robust contract enforcement provisions to allow the Department to demand documented evidence from PowerSchool demonstrating its compliance with the terms and conditions of the agreement.

iii. If it is not possible to review and renegotiate an agreement in a timely manner, pursuant to section 76(2) of the Act, I recommend the Department enter into an addendum to the Department's contract with PowerSchool, until such time as the agreement can be renewed or renegotiated.

iv. I recommend the Department limit access to its PowerSchool SIS through PowerSource, or any other remote maintenance support

connection, for only as long as necessary to provide the requested technical service.

v. I recommend the Department review PowerSchool's security and information management policies and procedures and associated documentation to ensure they address identified vulnerabilities that contributed to the PowerSchool breach.

vi. Pursuant to section 76(2) of the Act, I recommend the Department continue to take steps to standardize, define, and document its monitoring of security and auditing provisions under current and future agreements with PowerSchool, and obtain evidence of PowerSchool's fulfillment of its contractual obligations on an annual basis. This includes effective monitoring of PowerSchool's security measures in compliance with legal requirements, current industry standards, and best practices that are reasonable in the circumstances.

vii. Pursuant to section 76(2) of the Act, I recommend the Department take action to enforce its contractual provisions with PowerSchool, in the event PowerSchool does not comply with its contractual obligations to protect and secure personal information it processes.

viii. Pursuant to section 76(2) of the Act, I recommend the Department complete a comprehensive review of all open text fields in PowerSchool SIS to confirm their necessity and convert any required fields to standardized drop-down formats to ensure consistency and minimize unnecessary data collection.

ix. Pursuant to section 76(2) of the Act, I recommend that all fields identified as non-essential be immediately locked, with the Department reviewing existing entry information and permanently removing any information that is not required for operational or statutory purposes.

x. Pursuant to section 76(2) of the Act, I recommend that the Department update its existing privacy impact assessment on PowerSchool SIS, to reflect current practices and updates related to student personal information, inclusion of teacher personal information in its assessment, identification of open input fields as a risk and identification of measures being put in place to address this risk.

xi. Pursuant to section 76(2) of the Act, I recommend the Department develop comprehensive retention and destruction policies and procedures for all student records and teacher records, including records contained within PowerSchool SIS. Once developed, the Department should review the terms of its third-party services agreement and, if applicable, incorporate an ongoing retention and destruction schedule that the service provider must follow during the life of the contract.

xii. Pursuant to section 76(1)(a) of the Act, I recommend the Department stop collecting, using, or disclosing student MCP information.

xiii. Pursuant to section 76(1)(b) of the Act, I recommend the Department destroy and purge student MCP information from all student records[37], including but not limited to, destruction and purging of this information from PowerSchool SIS, electronic records, and paper records.

xiv. I recommend that the Department provide direct notification to the parents or guardians of the 14 currently enrolled students whose potential SIN information was taken in the breach.

---

[37] The Department describes the official repository of student records as a combination of: "(1) PowerSchool SIS, Review 360, and Responsive Teaching and Learning database electronic records; and (2) paper files stored in schools or an alternate location (active student files are maintained at the school the student is currently attending. Students who have graduated may have their file stored in an alternate location)", noting that every student would have a cumulative file and some students would also have a confidential file.

xv. Pursuant to section 76(2) of the Act, I recommend the Department clearly communicate in all of its future indirect notifications and subsequent notification updates, whether direct notification will be provided to all impacted individuals and, if not, the reasons why.

xvi. Pursuant to section 76(2) of the Act, I recommend the Department update its webpage to ensure accurate and accessible information, and I recommend that the Department clearly communicate in its FAQ section that not all impacted individuals will receive direct notification, and explain the reasons why.

xvii. Pursuant to section 76(2) of the Act, I recommend the Department follow up with PowerSchool to request information and evidence of actions PowerSchool committed to undertake as part of its Letter of Commitment with the Federal Privacy Commissioner's Office.

[171] As set out in section 77(2) of the **Access to Information and Protection of Privacy Act, 2015**, the head of the Department must give written notice of their decision with respect to these recommendations to the Commissioner within 10 business days of receiving this Report.

[172] Dated at St. John's, in the Province of Newfoundland and Labrador, this 11th day of May 2026.

Kerry Hatfield
Information and Privacy Commissioner
Newfoundland and Labrador

APPENDIX A – Timeline Summary of Implementation of PowerSchool

The following timeline is based upon the information that was provided by the Department as explanation of the implementation of PowerSchool SIS in Newfoundland and Labrador:

2010-2011

- PowerSchool was first brought into our province in 2010 as part of a test project by several schools in what was then known as the Central School District with multiple schools using the system by the end of 2011.

2012-2017

- By 2012, each of the four English school districts [Labrador School District, Western School District, Nova Central School District (also known as the Central School District), and Eastern School District] had their own instances of PowerSchool but not for all schools.
- In 2013, the four English school districts were merged into 1 district, the Newfoundland and Labrador English School District (NLESD) which took management of all four separate PowerSchool instances but kept them separate until 2016 when the four regional instances were combined into one NLESD instance.
- By 2017, all schools in the English school district were using PowerSchool.

2018 -2020

- In July 2018, the Department and the OCIO started a project [Student Administration and Certification System (SACS) project] to create a consolidated database of all K-12 students in the province and place ownership of the data under the control and direction of the Department.
    - The system would also provide the functionality related to High School Certification, replacing the existing High School Certification mainframe system. To accomplish this, PowerSchool SIS was expanded to include all students in the province, and modifications were made to accommodate the high school certification requirements. The OCIO project team and staff at the Department worked with NLESD and PowerSchool to build a customized PowerSchool cloud hosted SIS instance that would migrate existing PowerSchool data from the NLESD on-site server to the new Department instance.

2020-Current

- The Department activated its cloud-based single instance of PowerSchool SIS at the end of August 2020, and the NLESD server was shut down.
- As part of this project, the CSFP schools as well as all private and indigenous schools were added to the instance which meant that all students in the province were now included in PowerSchool SIS.

- The project also imported student records from 1995 to 2020 from the old Department High School Certification database (an on-premises data server of the OCIO).
- Since 2020, the Department has managed PowerSchool SIS with the support of the OCIO and NLSchools until NLSchools was incorporated into Department on January 1, 2024.

APPENDIX B – Student Input Fields in PowerSchool

Below is a list of PowerSchool input fields for student information that were being used in Newfoundland and Labrador at the time of the PowerSchool breach. Fields marked as "not on student table" are stored on data tables that were not impacted in the PowerSchool breach.

Student

Field	Comments
Student's Preferred Name	(Last, First, Middle) (3 fields total)
Student's Legal Name	(Last, First, Middle) (3 fields total, not on student table)
Home address Street	Apt/Suite (2 fields)
Home address City/Community	Province, Postal Code (3 fields)
Mailing address Street	Apt/Suite (2 fields)
Mailing address City/Community	Province, Postal Code (3 fields)
Home Phone	(XXX) XXX-XXXX
Age	
Gender	
Date of Birth	
MCP	
MCP Expiry Date	(not on student table)
French Program Type	(not on student table)
Type of Student	(not on student table)
Scheduling/Reporting Citizenship	(not on student table)
Self-identified Indigenous Status	(not on student table)
Student lives with	(not on student table)
Guardian email	
Parent/Guardian 1	(last, first)
Parent/Guardian 1 Home Phone	(XXX) XXX-XXXX (not on student table)
Parent/Guardian 1 Day Phone	(XXX) XXX-XXXX (not on student table)
Parent 1 Cell Phone	(not on student table)
Parent 1 email	(not on student table)
Parent/Guardian 1 Employer	(not on student table)
Parent/Guardian 2	(last, first)
Parent/Guardian 2 Home Phone	(XXX) XXX-XXXX (not on student table)
Parent/Guardian 2 Day Phone	(XXX) XXX-XXXX (not on student table)
Parent 2 Cell Phone	(not on student table)
Parent 2 email	(not on student table)
Parent/Guardian 2 Employer	(not on student table)
Contact #1	
Contact Name	(Last, First)
Relationship	(not on student table)
Phone	
Phone Type	(not on student table)
Contact #2	
Contact Name	(Last, First)

Relationship	(not on student table)
Phone	
Phone Type	(not on student table)
Contact #3	
Contact Name	(Last, First)
Relationship	(not on student table)
Phone	
Phone Type	(not on student table)
Allergies	(not on student table)
Special Medical Considerations	(not on student table)
Bus Route	
Bus Stop	
Student Alternate Transportation	(not on student table)
Type of Transportation	(not on student table)
Doctor	
Dentist	(not on student table)
Immunizations	(4 fields - not on student table)
Medical Alert Text	
Alert Expires	(date)
Student username	
Student password	(note this is an encrypted field and not readable)
Access ID	(for parent)
Access password	(for parent, one time registration code)
Other Alert Text	
Single Parent household	(dropdown, not on student table
Parent/Guardian is registered to receive	(5 check boxes, not on student table - Summary of Current Grades and Attendance, Detailed Report of Attendance, Detailed Report Showing All Assignment Scores For Each Class, School Announcements, Balance Alert Note Will Only Be Sent When a Student is Low o)
How often	(drop down box, not on student table)
Parent Guardian Alert	
Entry Date	
Code	
Exit Date	
Grade	
Exit Comment	
Entry Comment	
Full-Time Equivalency	
Track	
Region of District	
Exclude from the marks upload and course registration to the Department of Education	(check box - not on student table)
Community Service Hours Met	(check box - not on student table)

Student receives a student assistant	(not on student table)
Discipline Alert Text	
Alert Expires	

APPENDIX C – Teacher Input Fields in PowerSchool

Below is a list of PowerSchool input fields for teacher information that were being used in Newfoundland and Labrador at the time of the PowerSchool breach. Fields marked as "not on teacher table" are stored on data tables that were not impacted in the PowerSchool breach.

Teacher

Field	Comments
Teacher	
Name (Last, First MI)	(3 fields)
Preferred Name	
Email Address	
Title	
Teacher Number	
StatePrId	
Homeroom	
Home School	
Lunch ID	
Home Phone #	
School Phone #	
Street	
City, State, Zip	
DOB	
Staff Type	
Active	(check box)
Teacher Portal Username	
Teacher Portal Password	(note this is an encrypted field and not readable)
Home School / Current Assignment	
Sign in to PowerTeacher	(check box)
Teacher Username	
Teacher Password	(note this is an encrypted field and not readable)
Identity Provider Global ID	(not on the teacher table)
School affiliations	(4 fields per school assigned – home school, active, school and staff type)
Sign in to Administrative Portion of PowerSchool	(check box)
Admin Username	
Admin Password	(note this is an encrypted field and not readable)
Identity Provider Global ID	(not on the teacher table)
Default Group	
Allow Admin Sign in During These Times	(check boxes control 2 options, second option has 2 fields to allow range of times to be set)
Allowed Ips	
Roles and Schools	(not a field as such, multiple schools can be selected each with configurable roles, this is very complex section)