Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 092-2022

Living Sky School Division No. 202

February 1, 2023

Summary: The Living Sky School Division No. 202 (School Division) proactively reported a breach of privacy incident to the Commissioner when a work backpack was stolen from its Privacy Officer's vehicle. The Commissioner found that a privacy breach occurred. The Commissioner also found the School Division did not contain the privacy breach and that it did not take the necessary steps to properly notify the affected individual. The Commissioner further found the School Division conducted an adequate investigation into this privacy breach, but that it has not taken adequate steps to prevent future breaches. The Commissioner recommended that within 30 days of issuance of this Investigation Report, the School Division notify the affected individual, and that it finalizes its *Transportation of Records Protocol* (Protocol) and forwards it to all employees. The Commissioner added that the School Division should send yearly reminders to staff about the Protocol and make it part of new employee onboarding.

I BACKGROUND

[1] On May 13, 2022, Living Sky School Division No. 202 (School Division) reported the following breach of privacy to my office:

> Overnight on Friday, May 13, 2022 [School Division]'s privacy officer's vehicle was broken into. Part of what was stolen was the record for a … file with our office, along with [Privacy Officer] laptop and phone … The incident was reported to the police on the morning of Saturday, May 14, 2022.

[2] By email on May 25, 2022, my office notified the School Division that it would be undertaking an investigation into this matter.

[3] On June 29, 2022, the School Division provided my office with its response to the investigation.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[4] The School Division is a "local authority" pursuant to subsection 2(f)(viii) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). Therefore, I find I have jurisdiction to conduct this investigation.

2. Is personal information involved and did a privacy breach occur?

[5] In order for a privacy breach to occur, personal information as defined in subsection 23(1) of LA FOIP must be involved. Subsection 23(1) of LA FOIP provides an enumerated list of types of information that would qualify as personal information. However, the list is non-exhaustive. In order to qualify as personal information, there must be 1) an identifiable individual, and 2) the information must be personal in nature.

[6] The School Division stated there were paper documents of an employee from a file the Privacy Officer was working on that was included in what was stolen. The information, contained in a file, included the employee's first and last name, as well as data elements including the individual's employment history, opinions and/or views of the individual or others, and the individual's name combined with other information relating to them or that reveals information about them. As such, there is an identifiable individual involved and as other data elements are personal in nature, all constitutes personal information pursuant to subsections 23(1)(b), (f), (h), (k)(i) and (k)(ii) of LA FOIP, which provide as follows:

> **23**(1) Subject to subsections (1.1) and (2), **"personal information"** mean personal information about an identifiable individual that is recorded in any form, and includes:
>
> …

> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> …
> (f) the personal opinions or views of the individual except where they are about another individual;
>
> …
> (h) the views or opinions of another individual with respect to the individual;
>
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
>
> (ii) the disclosure of the name itself would reveal personal information about the individual.

[7] As the personal information was stolen, the disclosure of the personal information was not authorized. Therefore, I also find that a privacy breach occurred. The School Division does not deny this as it proactively reported the incident to my office. In the next section of this Investigation Report, I will consider the actions taken by the School Division to respond to the privacy breach.

3. Did the School Division respond appropriately to this privacy breach?

[8] As set out in my office's *Rules of Procedures*, when my office determines there has been a privacy breach, my office will analyze whether the local authority appropriately managed the breach by considering if it:

- Contained the breach (as soon as possible);
- Notified affected individuals (as soon as possible);
- Investigated the breach; and
- Taken appropriate steps to prevent future breaches.

[9] I will use these four steps to assess the School Division's response to the breach.

Contained the breach (as soon as possible)

[10] Soon after a local authority learns of a privacy breach, it should contain and recover any personal information that is involved. This will require determining how broad the privacy breach is and what type of records are involved.

[11] The School Division advised my office that it contacted the police and filed a police report in an attempt to contain the breach. On January 4, 2023, my office followed up with the School Division to see if any of the stolen items had been recovered. In response, the School Division advised:

> No, nothing has been recovered. In all honesty, the efforts made by the police seemed minimal at best and did not take advantage of opportunities presented to them. For instance, the cell phone was fully charged and could have been pinged for location, however the police indicated they would not take that step.

[12] In regard to the cell phone and laptop, the School Division advised:

> Specific to the laptop, the only files on the desktop had to do with non-people specific/related presentations on budgets, conflict resolution techniques and other HR areas of practice. All other files and programs are tied to the division's cloud service and not accessible due to:
>
> a) The password protection protocols, and
> b) The fact the device was immediately disabled and disconnected from our network by our IT team.
>
> As for the cell phone, it too was immediately disabled. I do not use it to text or in any other way use it beyond telephone and email. The only contacts on it were tied to the division's email so when we disabled that, nothing else existed. The disabling of both devices happened within 3 hours of my becoming aware of the break-in and would have been no more than 5 to 6 hours after the actual occurrence.

[13] On January 10, 2023, the School Division also advised of the following safeguards in place to prevent access by unauthorized individuals to the laptop and cell phone:

> The laptop requires a pin to access the desktop. If you want to access the network it requires a secondary Multi-Factor Authentications which changes frequently. The cellphone required recognition of my fingerprint [to gain access].

[14] I commend the School Division for disabling the cell phone and laptop immediately. It is also important to note that the School Division advised that the documents saved to the desktop did not contain personal information.

[15] The paper records containing personal information of an identifiable individual were not recovered by the School Division. Further, the School Division cannot confirm with absolute certainty that the information on the laptop or cell phone were not accessed prior to them being disabled. Therefore, I find the School Division did not contain the privacy breach.

Notified affected individuals (as soon as possible)

[16] Notice to affected individuals should happen as soon as possible when learning of a breach. Notifying an individual that their personal information has been inappropriately accessed or disclosed is important for a number of reasons. Not only do individuals have a right to know, but they also need to know in order to protect themselves from potential harm that may result from the inappropriate disclosure. Unless there is compelling reasons not to, local authorities should always provide notification.

[17] My office's *Privacy Breach Guidelines for Government Institutions and Local Authorities* (*Privacy Breach Guidelines*) suggests the following elements be included in notification to affected individuals on page 6:

- a description of the breach (a general description of what happened);
- a detailed description of the personal information involved (e.g. name, credit card numbers, medical records, financial information, etc.);
- a description of possible types of harm that may come to them as a result of the privacy breach;
- steps taken and planned to mitigate the harm and to prevent future breaches;
- if necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g. how to contact credit reporting agencies, how to change a health services number or driver's license number etc.);

- contact information of an individual within your organization who can answer questions and provide further information;
- a notice that individuals have a right to complain to the IPC (provide contact information); and
- recognition of the impacts of the breach on affected individuals and, an apology.

[18] In this matter, the School Division proactively reported this breach to my office. In addition, as the breach was a result of the Privacy's Officer's vehicle being broken into, the matter was reported to the police.

[19] The School Division advised my office that it did not notify the affected individual of this privacy breach. The School Division provided reasons why it did do so when providing my office its investigation details. However, my office was not satisfied with the School Division's explanation. Therefore, by email dated January 4, 2023, my office asked the School Division if it would reconsider notifying the affected individual. In its response, the school advised it would not.

[20] The reasons the School Division provided my office as to why it did not notify the affected individual appear to be more of an attempt to protect the School Division from the affected individual finding out about the breach of privacy. Its reasoning connects more to ongoing matters between the affected individual and the School Division, rather than how the breach of privacy could impact the individual.

[21] When assessing whether to notify an individual, a local authority should always take into consideration any risk to the individual of not notifying them. My office's *Privacy Breach Guidelines* discusses *significant risk of harm*:

> …both FOIP and LA FOIP require that, if there is an unauthorized use or disclosure of personal information, the government institution or local authority must notify the affected individual if the "incident creates a real risk of significant harm" to the affected individual (see sections 29.1 of FOIP or 28.1 of LA FOIP).

> What is a real risk of significant harm? For one, there must be some risk of damage, detriment, or injury to the individual that is significant in nature. In terms of PIPEDA amendments not yet in force, "significant harm" is described as follows:
>
> > 10.1(7) For the purpose of this section, "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.
>
> The second consideration is whether or not there is a "real risk" that the significant harm will occur. Probability of harm and sensitivity of the personal information must be considered in making this determination. The Alberta IPC, in its *Personal Information Protection Act Mandatory Breach Reporting Tool*, offers the following factors to consider in analyzing the circumstances surrounding the breach when making this call:
>
> - Who obtained or could have obtained access to the information?
>
> …
>
> - Is the information highly sensitive?
> - How long was the information exposed?
>
> …
>
> - Was the information recovered?
>
> [Emphasis added]

[22] Further, section 28.1 of LA FOIP lays out the requirement of a local authority to notify an individual if the privacy breach creates a real risk of significant harm to the individual. Section 28.1 of LA FOIP provides:

> **28.1** A local authority shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[23] First, it is not known who obtained access to the information as the documents were stolen and the School Division did not recover them. Second, the type of information that was contained in the paper documents that were stolen was sensitive information, as it involved an ongoing employment matter with the affected individual. It is possible that the stolen personal information could lead to reputational damage for the affected individual. Based

on all this, and what I outlined regarding risk, there is a real risk of significant harm to the individual.

[24] As such, I find the School Division has not notified the affected individual of this matter. I recommend the School Division notify the affected individual of this breach of privacy within 30 days of the issuance of this Investigation Report.

Investigate the breach

[25] Investigating the privacy breach to identify the root cause is key to understanding what happened. Identifying the root cause will help prevent similar breaches in the future. The internal investigation should also consider whether the safeguards that were in place at the time of the incident were adequate.

[26] The root cause of this privacy breach was due to the Privacy Officer leaving their work backpack in their vehicle. The Privacy Officer advised my office they did so as they were intending to travel with materials soon, and left them in their vehicle rather than taking the work backpack inside their home.

[27] The School Division's Privacy Officer advised they had taken training related to access and privacy in May 2022 – Managing Access and Privacy Programs (Advanced Course). I note the Privacy Office took this course a month before this incident occurred.

[28] Section 23.1 of LA FOIP requires a local authority to establish administrative, technical and physical safeguards to protect personal information. As outlined in my office's *Privacy Breach Guidelines*, *administrative safeguards* are controls that focus on internal organization polices, procedures, and maintenance of security measures that protect personal information. *Physical safeguards* are physical measures, policies, and procedures to protect personal information and related buildings and equipment from unauthorized intrusion and natural and environmental hazards. Examples include locked filing cabinets, offices and storage rooms, alarm systems, and clean desk approaches.

[29] In response to my office's follow up questions on this matter, on January 10, 2023, the School Division advised my office that at the time this breach occurred no policies or procedures existed in regard to leaving work in your vehicle. Further, the School Division advised:

> [School Division] is currently undergoing a full review, rewrite and rationalization of all procedures and protocols in every aspect of it's [sic] operations. Our review has uncovered that no current procedure or protocol addresses this item. Consultation is underway with our various groups to understand the realities of how they must operate relative to movement of electronic and hard copy data - that information will inform the drafting of a protocol which will be completed in the upcoming weeks….

[30] I do acknowledge that the School Division has in place technical safeguards, such as the requirement for two-factor authentication. In this matter, however, the School Division lacked proper administrative safeguards by not having a protocol in place for handling personal information. Further, the School Division lacked a policy regarding the physical transportation of personal information which would have required the Privacy Officer to take additional steps regarding transportation of personal information. Finally, it lacked physical safeguards when the Privacy Officer left the personal information and devices in an unattended vehicle.

[31] The School Division appears to understand it lacks proper protocols, and so I find the School Division conducted an adequate investigation into this privacy breach. I will discuss the School Division's mitigation efforts, including the pending policies and procedures in the next part of this report.

Prevent future breaches

[32] In responding to a breach of privacy, it is important that a local authority take steps to mitigate the risk of a similar breach occurring in the future. The following are some steps that can be taken:

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?

- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

[33] As noted above, the School Division did not have policies and procedures in place that specifically addressed taking work on the road or home and how to safeguard that work.

[34] When it provided my office its investigation details, the School Division advised:

> The situation was communicated to all leaders for awareness of break-in risks… A project team will be used to ensure we have fully scoped the opportunities.

[35] On January 29, 2023, the Privacy Officer emailed my office a copy of its proposed *Transportation of Records Protocol* (Protocol). In their email, the Privacy Officer stated:

> …We do not yet have organizational approval for it as one of our groups has highlighted the potential strain it puts on their methods of operation. These are our Learning Services personnel comprised of Occupational Therapists, Educational Psychologists, Speech/Language Pathologists. They have asked for time to consult with their colleagues in the Health Services world for how that sector might be addressing the question.
>
> I expect we will conclude on this item at our February 13 Governance Review and Approval session.

[36] As this incident occurred nine months ago, I am concerned the School Division has not acted more quickly to finalize its Protocol. Of heightened concern is that there are employees of a school division who are required to travel from school to school to perform their work duties. Therefore, I find the School Division has not taken adequate steps to prevent future breaches. I recommend that within 30 days of issuance of this Investigation Report, the School Division finalizes its Protocol and provides it to all employees.

[37] As the School Division finalizes its Protocol, I would like to draw its attention to my office's resource *Best Practices for Transporting Personal Information (PI) and Personal Health Information (PHI) Outside of the Office*. This resource outlines administrative,

physical and technical safeguards any organization should consider when developing policy and procedures for employees that transport personal information and personal health information outside of the office. The School Division may want to refer to this resource to ensure its Protocol captures all the necessary administrative, technical and physical safeguards. Once in effect, as a best practice the School Division should also review it annually with employees and make it part of new employee onboarding.

III FINDINGS

[38] I find I have jurisdiction to conduct this investigation.

[39] I find that a privacy breach occurred.

[40] I find the School Division did not contain the privacy breach.

[41] I find the School Division has not notified the affected individual of this matter.

[42] I find the School Division conducted an adequate investigation into this privacy breach.

[43] I find the School Division has not taken adequate steps to prevent future breaches.

IV RECOMMENDATIONS

[44] I recommend the School Division notify the affected individual of this breach of privacy within 30 days of the issuance of this Investigation Report.

[45] I recommend that within 30 days of issuance of this Investigation Report, the School Division finalizes its *Transportation of Records Protocol* and provides it to all employees.

Dated at Regina, in the Province of Saskatchewan, this 1st day of February, 2023.

Ronald J. Kruzeniski, K.C.
Saskatchewan Information and Privacy Commissioner