Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 033-2023, 042-2023

South East Cornerstone Public School Division No. 209

May 1, 2023

Summary: The South East Cornerstone Public School Division No. 209 (Cornerstone) proactively reported a privacy breach to the Commissioner. Cornerstone reported the loss of two students' cumulative files in a burglary that occurred at the post office, and that the students' files have not been recovered. Cornerstone notified the parents of the affected individuals of the privacy breach. The parents (Complainants) were not satisfied with Cornerstone's notification as they were concerned about the documents lost and requested that the Commissioner investigate. The Commissioner agreed that a privacy breach occurred as the disclosure was unauthorized, but Cornerstone did not cause it. The Commissioner recommended that Cornerstone update its administrative procedures to retain a copy of any records being transferred to another school and it investigate more efficient and lower risk options such as a secure electronic file transfer or consider using a courier to transfer records. The Commissioner also recommended that Cornerstone update its administrative procedures to track delivery of its packages and gather proof of delivery in a timely fashion.

I BACKGROUND

[1] On February 8, 2023, the South East Cornerstone Public School Division No. 209 (Cornerstone) proactively reported a privacy breach to my office, involving loss of two students' cumulative files. On the same day, Cornerstone provided notification to the parents of affected individuals as well. The affected individuals are two students who belonged to the same family.

[2] On February 22, 2023, my office received a complaint from the parents (the Complainants) of the affected individuals. On the same day, my office verified that the Complainants are

authorized to request this investigation on behalf of their children, who at the time were age 12.

[3] On February 23, 2023, my office notified the Cornerstone and the Complainant of my office's intention to undertake an investigation.

[4] On March 2, 2023, Cornerstone provided its completed "Privacy Breach Questionnaire", internal investigation report and supporting documents to my office. The Complainant did not provide any further information to my office.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[5] Cornerstone qualifies as a "local authority" pursuant to section 2(f)(viii) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). Therefore, I have jurisdiction to conduct this investigation.

2. Did a privacy breach occur?

[6] For LA FOIP to be engaged in a privacy breach, there must be personal information involved as defined by subsection 23(1) of LA FOIP.

[7] In this matter, Cornerstone identified the following data elements in the cumulative files: names, address, birth dates, student identification numbers, education programming including grades, attendance records and educational assessments. I note that Cornerstone's administrative procedures explain that cumulative files may also contain results of diagnostic testing (e.g., psychological reports, behaviour plans, etc.) and "all information affecting decisions pertaining to the education of a student…". These are data elements of personal information as defined by subsections 23(1)(a), (b), (c), (d), (e) and (k)(i) of LA FOIP, which provide as follows:

> **23**(1) Subject to sections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place or origin of the individual;
>
> (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;
>
> (c) information that relates to health care that has been received by the individual or to the health history of the individual;
>
> (d) any identifying number, symbol or other particular assigned to the individual;
>
> (e) the home or business address, home or business telephone number, fingerprints or blood type of the individuals;
> …
>
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
> …

[8] As the Complainant's children's personal information is involved, I find LA FOIP is engaged. The privacy rules outlined in Part IV of LA FOIP will guide this investigation.

[9] Once it has been established that personal information was involved, the next step is to consider if a privacy breach occurred. In this case, Cornerstone was sending the cumulative files (files) of the Complainant's children to a new school division as the family was moving. The files, however, were stolen from the post office on December 24, 2022, which means the files containing the personal information were intercepted and taken by those who stole it. Thus, a privacy breach occurred, but Cornerstone did not cause it. Cornerstone does not dispute this fact.

[10] I will move on to investigate the efforts Cornerstone made to address the privacy breach.

3. Did Cornerstone respond appropriately to the privacy breach?

[11] A privacy breach occurs where there is an unauthorized collection, use and/or disclosure of personal information. There are also other ways a privacy breach can occur (*Guide to LA FOIP*, Chapter 6, "Protection of Privacy", updated February 27, 2023, (*Guide to LA FOIP*, Ch. 6), p. 234).

[12] My office's *Rules of Procedure*, outlines that my office will analyze whether the local authority properly managed the privacy breach and took the following steps in responding:

- Contained the breach
- Notified affected individuals
- Investigated the breach
- Prevented future breaches

(*Guide to LA FOIP*, Ch. 6, p. 236)

[13] I will now consider each step individually and make any recommendation I may have at the end of this Investigation Report.

Contained the breach

[14] It is important to contain the breach immediately. In other words, ensure that personal information is no longer at risk. This may involve:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.
- Revoking access to personal information.
- Correcting weaknesses in physical security.

(*Guide to LA FOIP*, Ch. 6, p. 236)

[15] In its internal investigation report, Cornerstone explained it sent the files via registered mail, as per its internal policies and procedures, through Canada Post. A burglary occurred at the post office on December 24, 2022, and these files were part of the packages stolen from the post office. Cornerstone confirmed with my office that the post office reported this matter to the Royal Canadian Mounted Police (RCMP).

[16] At the time of writing this Investigation Report, my office checked and Cornerstone confirmed that the package containing the Complainant's personal information had not been recovered. As the files have never been recovered, I find that there is no containment.

Notified the affected individuals (as soon as possible)

[17] The following is a list of individuals or organizations that may need to be notified as soon as possible after learning of the incident:

- Your organization's privacy officer
- Office of the Information and Privacy Commissioner (IPC)
- The police, if criminal activity is suspected (e.g., burglary)
- The affected individuals

(*Guide to LA FOIP*, Ch. 6, pp. 237-238)

[18] LA FOIP requires that if there is an unauthorized use or disclosure of personal information, the local authority must notify the affected individual if the incident creates a "real risk of significant harm" to the affected individual. However, it is a best practice to provide notice in any breach situation. It is also best practice to contact the affected individuals directly, such as by telephone, letter, or in person.

[19] Notifications to affected individuals should include the following:

- 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 the affected individual because of the privacy breach.
- Steps taken and planned to mitigate the harm and 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).
- Contact information of an individual within the organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

[20] On February 8, 2023, Cornerstone provided notification to the Complainants and informed them of their right to request an investigation from my office. The letter also stated:

> …We sincerely regret to inform you that on February 6, 2023, we received notice that your children's cumulative records were stolen from the post office located in [name of town], SK during the night of December 24, 2022…
>
> These records contain personal information of your children including name, address, date of birth, student identification number, and reports relating to your children's educational programming. The post office has informed us that the theft was reported to the RCMP on December 25, 2022, however the records have not been recovered.
>
> In order to assist [name of new school division] with the continued education of your children, we are in the process of reproducing as many records as we can and will transfer these records to them as soon as possible.

[21] In its internal investigation report to my office, Cornerstone stated that it believed the level of harm was low, as this privacy breach may lead to possible humiliation. As such, it did not advise the Complainants on steps to mitigate the harm.

[22] As explained in my office's Investigation Report 218-2017 at paragraphs [6] and [31], Cornerstone should have considered that personal information of the affected individuals,

such as their names, date of birth, parents' names and contact details, speech assessment and reading assessment, etc., could leave these children and their parents vulnerable to identity theft. Loss of such personal information could lead to risk of physical or mental harm and risk of embarrassment, hurt, humiliation or damage of reputation. For more information, I encourage Cornerstone to refer to IPC Alberta's resource, "Key Steps in Responding to Privacy Breaches".

[23] Based on what Cornerstone included in its notification, I find that it could have provided more information to the Complainants in its notification regarding potential risks.

Investigated the breach

[24] Once a breach has been contained the next step is to investigate the breach. An investigation is a methodical process of examination, inquiry, and observation including interviewing witnesses and reviewing documents.

[25] Here are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach.
  - Has the privacy breach been contained.
  - What efforts has your organization made to contain the breach.

- What occurred
  - What type of breach occurred (e.g., collection, use, disclosure, accuracy, etc.).
  - What personal information was involved in the privacy breach.
  - When did the privacy breach occur? What are the timelines.
  - Where did the privacy breach occur.

- How did the privacy breach occur.
  - Who was involved.
  - What employees, if any, were involved with the privacy breach. What privacy training have they received.
  - Who witnessed the privacy breach.
  - What factors or circumstances contributed to the privacy breach.
  - What is the root cause of the breach.

- What is the applicable legislation and what specific sections are engaged.

- What safeguards, policies, and procedures were in place at the time of the privacy breach.

- Was the duty to protect met.
  - Were the safeguards, policies, and procedures followed.
  - If no safeguards, policies, or procedures were in place, why not.
  - Were the individuals involved aware of the safeguards, policies, and procedures.

- Who are the affected individuals.
  - How many are there.
  - What are the risks associated to a privacy breach involving this information (e.g., is the affected individual at risk for identity theft, credit card fraud, etc.).
  - Have affected individuals been notified of the privacy breach.

[26] Once the necessary information has been collected, it is a good idea to prepare an internal privacy breach investigation report. The report should include the following:

- Summary of the incident and immediate steps taken to contain the breach.

- Background of the incident, timelines, and a chronology of events.

- Description of the personal information involved and affected individuals.

- Description of the investigative process.

- The root and contributing causes of the incident.

- A review of applicable legislation, safeguards, policies, and procedures.

- Summary of possible solutions and recommendations for preventing future breaches. This should include specific timelines and responsibility for implementation of each action.

(*Guide to LA FOIP*, Ch. 6) pp. 238-239)

[27] Listed below is the timeline and summary of events provided by Cornerstone:

- December 21, 2022:
  - The student cumulative records for two students were sent via registered mail from a school (under Cornerstone) to the new school division.

- Week of January 30, 2023:

- The parent contacted the school principal to advise that the new school division had not received the student files.

- School checked Canada post tracking number, which indicated that the package had been delivered. A post office's employee informed the school that it had been quite some time that the new school division had picked its mail; and that the new school division had over fifteen parcels waiting for pickup at the post office.

- February 6, 2023:
  - The vice principal (VP) of the new school division contacted the principal of school to confirm that parcel from post office had been collected, but students' package was missing.

  - The VP explained that the postmaster informed that sometime in December, the post office had a break-in and suspected that this was one of the missing parcels. The post office had reported the burglary to the RCMP.

  - The school principal contacted the Cornerstone office to advise of the privacy breach.

- February 7, 2023:
  - The Privacy Officer initiated internal investigation and identified that the affected family was no longer registered with Cornerstone.

- February 8, 2023:
  - As the privacy breach occurred when records were in transit from Cornerstone to the new school division, Cornerstone proactively reported the privacy breach to the IPC and advised the family of the privacy breach.

[28] My office requested further information from the Cornerstone regarding contents and dates of documents from the students' missing files. Cornerstone listed the following documents and provided a blank/de-identified template used for each document:

Document	**Date**	**Status**
Student Registration Forms	2015	Missing
Cumulative Record Log	2015 to 2022	Missing
Acceptable Use Agreement (responsible use of technology and internet)	Unknown	Missing
Report Cards	2015 to 2022	Reproduced and provided to the family
Attendance Report	2015 to 2022	Reproduced and provided to the family

Speech and Language (SL) Assessment	June, 2022	Reproduced and provided to the family
Reading Assessment	April, 2022	Reproduced and provided to the family

[29] Cornerstone confirmed that it provided a paper and an electronic copy of records such as report cards, attendance report, SL assessment and reading assessment to the Complainants' children. It also provided a paper copy of these records to the new school division via registered mail again.

[30] With its internal investigation report, Cornerstone provided a copy of its Administrative Procedure 320 (AP-320), which discusses cumulative records extensively. I note that the AP-320 explains a cumulative record as below:

> Student records provide permanent, factual, objective and professional documentation of each student's attendance, academic progress, achievement reports, adaptations, specialized reports related to the student's educational program and personal demographic information. These records are confidential. They are used to provide a working profile of students who are enrolled in the school, and are used by the staff to help provide appropriate educational programming and supports for students from year to year. They are also valuable for assisting in the successful transition of students to another school. The cumulative record shall be the official working record for students currently enrolled in Division schools. Federal and provincial privacy and information sharing legislation have been followed in the creation, maintenance and use of cumulative records.
>
> All personal information is subject to the provisions of the *Local Authority Freedom of Information and Protection of Privacy Act* (LAFOIPP).

[31] Regarding responsibility for the cumulative record, AP-320 states:

> 2.3 When the Cumulative Record is transferred, responsibility for the record is also transferred.
>
> 2.4 A cumulative record file shall contain all information affecting decisions pertaining to the education of a student that is collected or maintained by the Division, regardless of the format in which it is maintained and stored (i.e., paper or electronic).

[32] Regarding requesting and transferring of the cumulative record, AP-320 states:

> 6.3.4 Upon receiving a request to transfer a cumulative record, the principal shall send the cumulative record using the most cost effective, secure method that will allow the package to be tracked. Options can include Registered Mail, Priority Post and Courier to the student's new school within three (3) working days.

[33] It appears that Cornerstone followed its administrative procedures to transfer the students' cumulative files to the new school division. As listed at paragraph [27] of this Investigation Report, Cornerstone tracked its steps for these file transfers, provided notifications and cooperated with the Complainants and the new school division to provide a copy of some of the lost records.

[34] This privacy breach occurred because the records were stolen from the post office and the school was not able to retrieve them. I am mindful that the circumstances are such that it was necessary for the RCMP to become involved as the matter relates to theft, and I am also mindful that no one would anticipate this type of theft occurring. Certainly, such a circumstance would be rare. Based on what Cornerstone provided, however, I am satisfied with the steps it took to investigate the privacy breach.

Prevented future breaches

[35] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring.

- What steps can be taken to prevent a similar privacy breach.
  - 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.

[36] My office inquired and Cornerstone confirmed that it did not keep a copy of the cumulative record log. As such, Cornerstone was unable to generate a copy of all the missing records. I note that while no public body can anticipate a burglary leading to a privacy breach; however, as a best practice, Cornerstone could retain a copy of all records being transferred to another school. This would help identify all records/personal information involved in a

situation and help it reproduce the records, especially if containment became an issue (see Investigation Report 154-2022 and Investigation Report H-2011-001).

[37] While I find Cornerstone's investigation was adequate, I find it could take additional steps to be able to account for lost records and to improve its procedures to help prevent a similar occurrence in the future. I recommend that Cornerstone update its administrative procedures to retain a copy of any records being transferred to another school.

[38] In its internal investigation report, Cornerstone stated that it followed its administrative policy by sending the packages to the new school division via registered mail, and the cause of the privacy breach was burglary. What also was a concern is the length of time the registered mail package was left at the post office and the lack of follow-up by Cornerstone to ensure it was delivered.

[39] In a similar incident, Nunavut IPC's Report 23-240-RR, the Commissioner commented on "using registered mail", as follows:

> [28] The principal benefit of using registered mail is that it provides proof of delivery into the hands of the addressee. (It also offers tracking, but that feature is available for some non-registered mail too.) A piece of registered mail is supposed to be handed over only if the addressee, showing proof of identity, signs for it. The addressee's signature is then available to the sender as proof of delivery.
>
> [29] **The evidence before me indicates, however, that nobody in HR was tracking the envelope's progress. Nobody in HR knew that the letter was taking a slow wander across southern Canada. Nobody in HR was checking to see if or when the Complainant signed for the letter. The benefit of using registered mail appears to have been lost.**
>
> [30] **It is possible there is a belief within HR that registered mail is more secure than other delivery methods. But there is nothing inherently secure about registered mail. Before the addressee signs for it, a registered letter is as subject to loss, damage, or theft as any other letter.**
>
> [31] **Although the privacy breach in this case was not HR's responsibility, I suggest that HR consider whether registered mail continues to meet the "reasonable security arrangements" standard in section 42 of the ATIPPA. There are electronic delivery methods that can provide proof of receipt and security of**

> **access. They are also much faster. Perhaps it is time for HR to re-think the use of registered mail as its preferred delivery method.**
>
> [Emphasis added]

[40] Similarly, to possibly avoid a privacy breach of this nature from occurring in the future, I encourage Cornerstone to investigate more efficient and lower risk options such as using a secure electronic file transfer or consider using a courier to transfer records of such sensitive nature.

[41] I acknowledge that Cornerstone followed the administrative procedures it had in place at the time; however, these could be further finetuned by including, as part of the procedure, that someone is responsible to follow-up with the receiving school when the package is expected to arrive. Therefore, I recommend that Cornerstone update its administrative procedures to track delivery of its packages and gather proof of delivery in a timely fashion.

III FINDINGS

[42] I find that I have jurisdiction to conduct this investigation.

[43] I find that the Complainant's personal information is involved pursuant to subsections 23(1)(a), (b), (c), (d), (e) and (k)(i) of LA FOIP.

[44] I find that a privacy breach occurred.

[45] I find that there was no containment.

[46] I find that Cornerstone could take additional steps to provide adequate notification.

[47] I find that Cornerstone conducted an adequate investigation.

[48] I find that Cornerstone could take additional steps to account for lost records.

[49] I find the Cornerstone could use more efficient and lower risk options such as secure electronic file transfer or consider using a courier to transfer records.

[50] I find that Cornerstone could take additional steps to confirm delivery of its package.

IV RECOMMENDATIONS

[51] I recommend that Cornerstone update its administrative procedures to retain a copy of any records being transferred to another school.

[52] I recommend that Cornerstone investigate more efficient and lower risk options such as using a secure electronic file transfer or consider using a courier to transfer records.

[53] I recommend that Cornerstone update its administrative procedures to track delivery of its packages and gather proof of delivery in a timely fashion.

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

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