Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 200-2023

South East Cornerstone Public School Division No. 209

February 1, 2024

Summary: The South East Cornerstone Public School Division No. 209 (School Division) proactively reported a privacy breach to the Commissioner's office. The report stated that an unauthorized third party had gained access to three of its systems and uploaded data, including personal information, to a cloud storage service. The Commissioner investigated the incident under *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). He found that there was a privacy breach involving personal information. He found that the School Division took appropriate action to contain the breach, notify affected parties and investigate the breach. However, he found that the School Division could take additional steps to prevent further breaches. The Commissioner recommended that the School Division continue to conduct dark web monitoring for five years and notify affected individuals of any evidence of activity relating to them on the dark web. He also recommended that if the School Division discovers an individual's information on the dark web, it continues the credit monitoring services for a minimum period of five years from the date the information is discovered. The Commissioner made several recommendations relating to additional measures to prevent further breaches.

I BACKGROUND

[1] This Investigation Report considers a privacy breach that was proactively reported to my office on August 8, 2023, by the South East Cornerstone Public School Division No. 209 (School Division).

[2] The School Division reported that a breach occurred when three of its IT systems were accessed by an unauthorized third party on February 8, 2023. While no malware was

detected within the system, a total of eight "archive files" were identified as having been exfiltrated or removed from its network. The unauthorized party moved the data to a third-party cloud storage provider. The School Division estimated that 20,000 people were affected by the breach.

[3] On September 9, 2023, my office notified the School Division that it would be conducting an investigation into the privacy breach. On October 23, 2023, the School Division provided my office with its completed *Privacy Breach Investigation Questionnaire* (Questionnaire).

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[4] The School Division qualifies as a "local authority" pursuant to subsection 2(1)(f)(viii) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

[5] As set out in my office's *Guide to LA FOIP*, Chapter 6, "Protection of Privacy" (*Guide to LA FOIP*, Ch. 6) at page 39, the privacy rules in LA FOIP only apply to personal information. Therefore, I must determine if the information at issue qualifies as personal information under subsection 23(1) of LA FOIP.

[6] The School Division stated that it was unable to definitively determine what information was impacted by the incident. However, it asserted that the information inappropriately accessed varied with each affected individual. It asserted that the information may have included the names and contact details of former and current employees, students and parents. In the case of some of its employees, social insurance numbers and banking information may have been impacted. In the case of parents and students, information impacted may have included dates of birth, gender, health card numbers, allergy information, student numbers, achievements and grades.

[7] Individuals' names and personal contact details would qualify as personal information pursuant to subsection 23(1)(e) of LA FOIP. Individuals' social insurance numbers and health card numbers would qualify as personal information pursuant to subsections 23(1)(d) and (k) of LA FOIP. Employment, financial, banking and education related information would qualify as personal information under subsection 23(1)(b) of LA FOIP. Information about the individuals' family members, gender, and place and date of birth would qualify as personal information pursuant to subsection 23(1)(a) of LA FOIP. Information about students' allergies would qualify as information about their health history pursuant to subsection 23(1)(c) of LA FOIP.

[8] These subsections provide as follows:

> **23**(1) Subject to subsections (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 of 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 or fingerprints or blood type of the individual;
>
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or

[9] Given the nature of the information the School Division believed was involved, I find that the information qualified as personal information pursuant to subsections 23(1)(a), (b), (c), (d) and (k) of LA FOIP.

[10] As the School Division is a local authority, and personal information is involved in this breach, I find that I have jurisdiction to investigate under LA FOIP.

[11] The School Division has acknowledged that a privacy breach occurred. Therefore, I now turn to consider if it appropriately responded to the breach.

2. Did the School Division respond appropriately to the privacy breach?

[12] In circumstances where there is no dispute that a privacy breach has occurred, my office's investigation focuses on whether the local authority has appropriately handled the breach.

[13] As set out in section 4-4 of my office's *Rules of Procedure* and my office's *Guide to LA FOIP*, Ch. 6 at page 235, my analysis of the School Division's responses to the privacy breach looks at its efforts to:

1. Contain the breach
2. Notify affected individuals
3. Investigate the breach
4. Prevent future breaches

[14] I turn to consider if the School Division appropriately addressed each of these steps.

Contain the breach

[15] My office's *Guide to LA FOIP*, Ch. 6 at page 235, states that upon learning that a privacy breach has occurred, local authorities should immediately take steps to contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that has been breached.

- Revoking accesses to personal information or personal health information.
- Correcting weaknesses in physical security.

[16] In my office's Investigation Report 197-2022, 215-2022, I stated that in assessing efforts to contain the breach, my office applies a reasonableness standard. We want to have some reassurance that the institution has reduced the magnitude of the breach and the risk to affected individuals.

[17] The following timeline of key events is based on information provided by the School Division:

- February 8, 2023 – The School Division's IT personnel discovered that an unauthorized third party had accessed its network and was in the process of copying data to a third-party cloud storage service.
- February 8, 2023 – IT personnel notified the School Division's privacy officer. The School Division notified the Ministry of Education.
- February 8, 2023 – The School Division immediately deployed counter measures to protect the network from further unauthorized accesses including by isolating systems and restricting remote connections to the network.
- February 9, 2023 – The School Division engaged third-party cybersecurity experts and external breach counsel to assist in further containing, investigating and recovering from the incident.
- February 10, 2023 – The School Division notified the RCMP National Cybercrime Coordination Centre.
- February 10, 2023 – Notice of the incident was provided to all staff members and parents/guardians of students currently enrolled in the School Division's schools.
- February 18, 2023 – The third party cloud storage service confirmed that all accounts associated with the incident and the School Division's data had been "permanently suspended."
- February 22, 2023 – The third party cybersecurity expert advised that the incident was contained.
- March 21, 2023 – The School Division sought a second opinion regarding the "specifics of exfiltration archives" or, in other words, the information impacted by the breach.

- May 29, 2023 – The School Division was advised by its second cybersecurity expert, that further specifics of files and information impacted by the breach could not be obtained given the available evidence.

- June to August 2023 – The School Division conducted "extensive reviews" of the affected systems. This included efforts to identify the information affected. The School Division identified three systems which contained information that was accessed. No malware was detected within the system. A total of "eight archive files" were identified as having been exfiltrated from the network.

- August 28, 2023 – The School Division notified potentially affected individuals by letter and indirectly by posting a notice on its website.

[18] The School Division further explained that to contain the breach it:

- deployed a leading endpoint detection solution across all workstations and servers in the environment and actively monitored for evidence of ongoing compromise or unauthorized access;

- conducted an organization-wide user credential reset;

- implemented geo-fencing to block foreign connections;

- implemented multi-factor authentication for VPN, Microsoft Office 365 and IT domains; and

- ensured systems and applications were appropriately patched and hardened against known vulnerabilities.

[19] In its Questionnaire, the School Division stated:

> Unless a separate copy was taken, it is possible that the third party behind this incident lost access to the data as soon as the accounts were suspended.

[20] The School Division took timely and appropriate steps to contain the breach. Despite the risk that the third party may have taken a copy of the information, the School Division's efforts reduced the magnitude of the breach and the risk to individuals. Therefore, I find that the School Division contained the breach.

[21] The School Division stated that it actively monitored the dark web "during the incident response" and since then it has retained a monitoring service to continue monitoring the

dark web. As of the date of this breach report, it had not found any evidence to suggest that the information had been published.

[22] In previous investigations, such as Investigation Report 089-2021, et al, I have recommended that public bodies monitor the dark web for a period of five years. Given the risk that the third party may have copied the information, I will follow the same approach here. I recommend that the School Division continue to conduct dark web monitoring for five years from the date of the privacy breach. I also recommend that the School Division notify any affected individuals of any evidence of activity relating to them on the dark web.

Notify affected individuals

[23] Section 28.1 of LA FOIP requires local authorities to notify individuals when their personal information has been breached and a real risk of significant harm exists for the affected individuals.

[24] Section 28.1 of LA FOIP states:

> **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.

[25] As stated in my office's *Guide to LA FOIP*, Ch. 6 at page 231, even where section 28.1 of LA FOIP does not apply, unless there is a compelling reason not to, local authorities should always notify affected individuals of a privacy breach.

[26] As noted above, the School Division stated that it cannot be certain as to the number and identity of the affected individuals. It estimates that 20,000 people were impacted. It added that it "provided preliminary notice of the incident to its employees and parents/guardians of all active students" on February 10, 2023 – two days after discovery of the breach.

[27] The preliminary notice provided to parents and students on February 10, 2023, stated that "there is currently no indication that any personal information" has been impacted. The notice provided to current staff stated that employees should be "aware of the possibility that some employee data may have been impacted."

[28] The School Division advised my office that it also notified its privacy officer and the RCMP on February 10, 2023.

[29] The School Division asserted that on August 28, 2023, it provided a detailed notice to all individuals it believed may have been affected by the breach. This included former staff, current staff, and current parents and students. Former students were notified by a posting on the School Division's website. My office was notified on the same day.

[30] It is important to notify affected individuals for several reasons. Affected individuals have a right and need to know to protect themselves from any harm that may result. Local authorities may also want to notify organizations, such as, my office, law enforcement or other regulatory bodies that oversee professions.

[31] My office's *Guide to LA FOIP*, Ch. 6 at page 231 sets out the information that should be included in every notice to affected individual(s):

- 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 information;

- A notice that individuals have a right to complain to my office (provide contact information); and
- Recognition of the impacts of the breach on affected individuals and, an apology.

[32] The School Division provided my office with copies of the preliminary and final notices sent to the affected parties.

[33] I note that the August notification letters included all the elements described above in paragraph [31]. The notification letters that were sent to staff and former staff also included a warning about the risk of identity theft and set out the actions that individuals could take to mitigate the risks. These letters included offers to provide credit monitoring and detailed information about how to apply for that service. In response to questions posed by my office, the School Division stated that the credit monitoring was offered for one year.

[34] As the personal information at issue for staff and former staff may have included social insurance numbers and banking information, the School Division took appropriate action by offering credit monitoring.

[35] In the previous reports where identity theft has been a risk, such as my office's Investigation Reports 370-2021 and 061-2023, 087-2023, I have found public bodies should offer affected parties credit monitoring for a minimum of five years. The School Division asserted that its decision to provide credit monitoring for one year only took into account the risk to individuals, market standards and the sensitivity of the information. It added that there was no way to determine if any personal information was "actually compromised" in relation to the incident despite considerable efforts.

[36] When asked by my office, the School Division stated that, as of the date of this Investigation Report, it had not received any information or allegations from affected parties regarding identity theft or fraud.

[37] In my view, the personal information potentially at risk here was sensitive and was sufficient to pose a risk of identity theft. However, given the information provided, the

circumstances of this breach and the continued efforts by the School Division to monitor the dark web, I am satisfied that one year of credit monitoring is sufficient.

[38] I recommend that if the School Division discovers an individual's information on the dark web, it should continue credit monitoring for a minimum period of five years from the date their information is discovered on the dark web. This is consistent with the approach taken in previous investigation reports, including Investigation Report 009-2020, et al.

[39] Regarding the timing for its notification, based on the information provided, it is apparent that the forensic investigation by the first expert retained by the School Division was completed on March 21, 2023. Another cybersecurity expert was retained to validate the first firm's findings and that the files or information exfiltrated could not be identified. The experts both concluded that there was insufficient evidence to identify the specific files or information involved. This work was competed at the end of May 2023.

[40] Given that the School Division was not able to determine the "specifics of the exfiltrated archive files" from the work of its experts, it explained:

> SECPSD set about reviewing and analyzing the information on systems identified as having been accessed, including various file directories the copied data is believed to have originated from. That process took some time to complete given the volume of data maintained on those systems, hence the additional time and effort SECPSD expended at the outset to identify what information was compromised specifically. SECPSD notified all potentially impacted individuals as soon as possible once its review and analysis was complete.

[41] Consequently, the School Division's detailed notice to affected parties was not sent until August 28, 2023, over six months following the breach. I commend the School Division for providing a preliminary notice to some affected parties at the earliest opportunity even though it did not have all of the information about the data that was exfiltrated. I also commend the School Division for notifying former students via a website posting. In light of the information provided by the School Division about the complexities of the investigation, I find that the notice to affected parties was adequate.

Investigate the breach

[42] After containing the breach and notifying affected parties, local authorities should conduct an internal investigation. My office's *Guide to LA FOIP*, Ch. 6 at page 239, describes an internal investigation as a methodical process of examination, inquiry, and observation including interviewing witnesses and reviewing documents. The purpose is to conduct a root cause analysis, which is a useful process for understanding and solving a problem, and to identify measures necessary to prevent further similar breaches.

[43] The *Guide to LA FOIP*, Ch. 6 at page 239 states that a root cause analysis seeks to identify the origin of a problem by using a specific set of steps and tools to:

- Determine what happened,
- Determine why it happened, and
- Figure out what to do to reduce the likelihood that it will happen again.

[44] A root cause analysis should include a consideration of section 23.1 of LA FOIP. Section 23.1 of LA FOIP sets out the local authority's duty to protect personal information. This requirement includes establishing policies and procedures to maintain administrative, technical and physical safeguards. That provision states:

> **23.1** Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

[45] "Administrative safeguards" are defined in my office's *Guide to LA FOIP*, Ch. 6 at page 98, as controls that focus on internal organization policies, procedures, and maintenance of security measures that protect personal information. Examples include written policies and procedures, annual training for employees, confidentiality agreements, agreements with information management service providers, auditing programs, records retention and destruction schedules and access restrictions.

[46] "Technical safeguards" are defined in the *Guide to LA FOIP*, Ch. 6 at page 103, to mean the technology and the policy and procedures for its use that protect personal information and control access to it. Examples of technical safeguards include separate user identifications, passwords, firewalls, identification and authentication controls, virus scanners and audit capabilities in digital systems.

[47] As to the root cause of the breach, the School Division stated that the user credentials for an employee who was on a leave of absence were compromised. However, it does not know how those credentials became compromised despite the forensic investigations it conducted, including its examination of the laptop used by the employee. It added that its forensic experts believed that the incident "appeared to be a precursor to a ransomware attack based on their experience with similar matters and common indicia of such attacks."

[48] In response to questions from my office, it explained that there was no evidence that phishing was involved in this breach and there was no evidence that the employee's device was lost or accessed.

[49] It stated that the technical safeguards in place at the time of the breach included an endpoint security platform; multi-factor authentication for all staff user accounts; pre-screening of emails for potentially malicious attachments and links; installation of critical and high-severity patches within one month; continuous employee cyber awareness and phishing training; network detection response; and mandatory 90-day password resets for all staff.

[50] In response to questions from my office, it added that the School Division uses segregation to protect the systems in its network; however, at that time it did not have access rules in place to prevent lateral movement from within the system. The School Division does not believe that further segregation would have prevented the compromise of multiple accounts. Since the breach, it has made changes to its network configuration.

[51] The School Division also stated that there was no evidence that its monthly practice of updating and patching was not followed.

[52] The School Division provided my office with copies of the four policies in place to protect personal information at the time of the breach. The policies were entitled, "Responsible Use of Technology and the Internet", "Portable Technology Security", "Guidelines for Protecting the Privacy and Confidentiality of Personal information" and "Information Systems Security Procedures."

[53] Regarding these administrative controls, the School Division stated that the policies and procedures were followed. Other than its decision to change the password requirements from eight characters to 12, it is not proposing any changes to its policies.

[54] Based on a review of the policies provided to me, it appears that detailed requirements for the use of a strong password were not documented.

[55] In its "Information Systems Security Procedures", there is a requirement for students to change passwords every year and for staff to change it every 90 days. The "Portable Technology Security" policy states that "password protection mechanisms" available on portable technology must be activated to the greatest extent possible and "industry standards are to be deployed in the selection of appropriate passwords". The "Responsible Use of Technology and the Internet" policy does not address passwords. The School Division's "Guidelines for Protecting the Privacy and Confidentiality of Personal Information" policy states that technology should be "password-controlled and timed out when not in use."

[56] As noted in my office's, "Helpful Tips for Mobile Device Security"

> The use of passwords is a basic security measure that should be taken. Strong passwords are comprised of at least eight characters, with 14 or more being the ideal. They can include a combination of upper and lower case letters, numbers and symbols, rather than dictionary words. Avoid using predictable passwords like birthdates, favorite sports teams or easy-to-guess dictionary words like "password" or "Letmein". However, password phrases can be very good for example, "IwenttoballetinReginaon7thAve."

[57] The requirements for staff, parents and students to have strong passwords should be set out in clear written and enforceable policies and procedures. There should be measures in place to ensure that staff, parents and students are trained and informed about the policies and procedures.

[58] As noted above, the School Division stated that its password policy has been "updated" to require 12 characters instead of eight. I commend the School Division for taking this action. However, it did not provide my office with a copy of the new policy. Nor did it provide any information about its plan to implement and provide training on the new policy.

[59] I am concerned about the fact that the credentials that were used in this case belonged to an employee who was on leave for a period of 11 months. When I asked the School Division to explain why this person's credentials remained active during the period of the leave, I was informed that the employee needed access to the system via their laptop computer to coach basketball. I was not provided with any details such as what parts of the system the employee needed access to.

[60] The School Division stated that there is currently no policy in place that deals with leaves and access to IT systems. I will consider this further below in my analysis of the steps taken to prevent further breaches.

[61] I find that the School Division completed an investigation into the breach.

Take appropriate steps to prevent future breaches

[62] Once local authorities contain a breach and identify a root cause, they should consider and implement solutions that help prevent the same type of breach from occurring again. Prevention is one of the most important steps. A privacy breach cannot be undone but a local authority can learn from one and take steps to help ensure that it does not happen in the future.

[63] To prevent future breaches, the School Division decided to continue the use of the end-point detection response tool which it deployed immediately following discovery of the breach. It has also acquired a security operations centre, managed detection and response risk services with a third party vendor. As noted above, it has also "updated its password policy" so that staff and students are now required to use a 12-character password, instead of eight.

[64] When asked what additional safeguards are needed, the School Division stated that it is investigating a zero-trust network access solution that assumes that no user or device inside or outside the network is trusted by default. It also requires verification for every user and device accessing resources on a private network. I recommend that, within 30 days of issuance of this Investigation Report, the School Division complete its investigation into acquiring a zero-trust network access solution.

[65] The School Division stated that at the time of the breach, it had in place requirements for multi-factor authentication for all staff who were accessing the systems off premises. Since the breach, the School Division has restricted off premises access to all internal applications.

[66] I find that the proposed steps to be taken by the School Division to prevent future breaches are appropriate. However, it could do more.

[67] In recent years, there have been a spate of data breaches involving school boards in Canada (See for example, reports of breaches within British Columbia's Maple Ridge-Pitt

Meadows School District, and Ontario's Huron-Superior Catholic School Board and Durham District School Board). According to a December 2020 article in "Canadian Security Magazine", these types of attacks are on the rise. It added:

> Given the large number of users, school networks have many vulnerable points of entry and face higher risks of malware infection and transmission. Students might also use devices with outdated software, and their home networks might be insecure. If one student's device is attacked, that may be used as an entry point to attack the entire school network.

[68] Parents and students did not have access to the systems affected by this breach; however, the risk of malware remains high. School Divisions must ensure that they have measures in place that are reasonable based on what appears to be a growing risk and the sensitivity of the information involved.

[69] The School Division should ensure that password policies aimed at staff, parents and students are documented. The policies should provide clear, detailed and audience appropriate instructions and training about the requirements for a strong password, including the types and number of characters required to comprise the strong password. I recommend that, within 30 days of issuance of this Investigation Report, that the School Division develop and implement a password policy.

[70] The School Division should develop a policy that governs staff access to its IT systems when they are on a leave of absence. The policy should ensure that staff are only given access to the information that is reasonably necessary to carry out any school approved duties or functions.

[71] In arriving at the appropriate policy, the School Division should be aware of its obligations of data minimization. "Data minimization" is defined in my office's *Guide to LA FOIP*, Ch. 6 at pages 24 to 25, as a rule requiring an organization to always collect, use, and disclose the least amount of personal information necessary for the purpose. The exercise of collecting, using, and disclosing personal information is always subject to the data minimization principle. I recommend that, within 30 days of issuance of this Investigation

Report, the School Division develop and implement a policy on access to the School Division's systems by staff who are on leave.

[72] I note that some of the records involved in this incident were quite old. Records of former staff dated back to February 2010, records of parents dated back to September 2013 and records of students dated back to September 1997. The School Division stated that the records were retained in accordance with records retention schedules in place that were developed by the Saskatchewan School Boards Association.

[73] It appears that in some cases the records retention schedule may not have been complied with. For example, some of the records relating to students are required to be retained for a period of 25 years. If the oldest student records in the School Division's systems dated from September 1997, it appears that some records may have been retained two years longer than the 25-year period set out in the retention schedule. Timely and appropriate secure destruction of records is an important measure to reduce the impact of a privacy breach.

[74] I recommend that, within 30 days of release of this Investigation Report, the School Division complete a review of its record holdings involving personal information and applicable retention schedules to determine if it is in full compliance with the schedules.

[75] Training is an important administrative control. The School Division stated that all staff are provided security training through a third party vendor. It described this as "continuous awareness and phishing training." It is not clear what the School Division means by "continuous." The School Division also stated that its Information Systems staff regularly participate in online and in person security training.

[76] Security training, like privacy training, should be mandatory and be refreshed annually. I recommend that, within 30 days of issuance of this Investigation Report, the School Division review its policies and practices and take steps to ensure that its security training is provided, at a minimum, annually, and it is mandatory for all staff.

[77] For all of these reasons, I find that the School Division's plans to prevent future breaches could include some additional steps.

III FINDINGS

[78] I find that I have jurisdiction to investigate this matter under LA FOIP.

[79] I find that a privacy breach occurred.

[80] I find that the School Division contained the breach.

[81] I find that the School Division's notices to the affected parties were adequate.

[82] I find that the School Division conducted an investigation into the breach.

[83] I find that the School Division's plan to prevent future breaches of this nature could include some additional steps.

IV RECOMMENDATIONS

[84] I recommend that the School Division continue to conduct dark web monitoring for five years from the date of the privacy breach.

[85] I recommend that the School Division notify affected individuals of any evidence of activity relating to them on the dark web.

[86] I recommend that if the School Division discovers an individual's information on the dark web, it should continue credit monitoring for a minimum period of five years from the date their information is discovered on the dark web.

[87] I recommend that, within 30 days of issuance of this Investigation Report, the School Division complete its investigation into acquiring a zero-trust network access solution.

[88] I recommend that, within 30 days of issuance of this Investigation Report, that the School Division develop and implement a password policy.

[89] I recommend that, within 30 days of issuance of this Investigation Report, the School Division develop and implement a policy on access to the School Division's systems by staff who are on leave.

[90] I recommend that, within 30 days of release of this Investigation Report, the School Division complete a review of its record holdings involving personal information and applicable retention schedules to determine if it is in full compliance with the schedules.

[91] I recommend that, within 30 days of issuance of this Investigation Report, the School Division review its policies and practices and take steps to ensure that its security training is provided, at a minimum, annually, and it is mandatory for all staff.

Dated at Regina, in the Province of Saskatchewan, this 1st day of February, 2024.

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