Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 031-2020

Chinook School Division No. 211

August 11, 2021

Summary: The Chinook School Division No. 211 (School Division) proactively reported a breach of privacy to the Commissioner advising that a GitHub code repository was set to public instead of private for approximately 36 hours. The Commissioner found that a privacy breach occurred and that the School Division properly contained the breach of privacy. The Commissioner further found that the School Division did not provide proper notification of the breach and it failed to meet its duty to protect pursuant to subsection 23.1 of *The Local Authority Freedom of Information and Protection of Privacy Act*. Finally, the Commissioner found that although the School Division appropriately investigated the breach, it did not provide enough details of how it will prevent future breaches of GitHub or similar applications. The Commissioner recommended the School Division provide notification of this breach to all affected individuals. The Commissioner also recommended that the School Division implement a security assessment and ongoing security review process for new and existing applications, including GitHub.

I BACKGROUND

[1] On February 4, 2020, the Chinook School Division No. 211 (School Division) proactively reported the following breach of privacy incident to my office:

> On Jan 28, 2020, a GitHub code repository (repo) was set to be public instead of private. The code contained a CSV (schoolmessenger.csv) file that included 2841 records….

[2] On February 6, 2020, my office notified the School Division that we were opening a file on this matter and asked the School Division to forward its internal investigation report.

[3] Upon review of the School Division's internal investigation report, my office advised the School Division that due to the number of affected individuals, my office would be conducting a formal investigation and issuing a report on this matter.

II DISCUSSION OF THE ISSUES

1. Is *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) engaged and do I have jurisdiction to investigate this matter?

[4] The School Division is a "local authority" pursuant to 2(f)(viii) of LA FOIP. Therefore, I have jurisdiction to investigate this matter.

[5] In a breach of privacy investigation, in order for LA FOIP to be engaged, there must be personal information as provided for in subsection 23(1) of LA FOIP. To qualify as personal information, the information must relate to an identifiable individual and the information must be personal in nature.

[6] The School Division advised my office that the following data elements were involved for 2,841 student records:

- student name(s);
- student identification (ID) number;
- telephone numbers;
- school code;
- grade; and
- parent email address.

[7] These data elements qualify as personal information pursuant to subsections 23(1)(b), (d), (e), (k)(i) and (ii) of LA FOIP, which provide:

> **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:
>
> …

> (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;
>
> …
> (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 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.

[8] Therefore, as there is personal information involved, LA FOIP is engaged in this matter.

2. Did a privacy breach occur?

[9] Through a review of the School Division's investigation report, the following occurred between January 28, 2020 at 9:16am and January 29, 2020 at 10:58pm:

- A GitHub code repository was moved from an existing personal repository into a new business repository. The new repository access settings were automatically set to public and not discovered as the personal repository had private access and therefore, it was thought the new repository would be set to the private access as well.
- The breach was discovered on January 29, 2020 when [Outside Organization] (where two parents in the School Division worked) performed a routine deep web internet crawl while looking for any references to [Outside Organization]'s domain. A staff member with [Outside Organization]'s IT staff took a screenshot of its domain related data and shared it with their internal privacy officer. The two parents were informed their work email addresses were available.
- The breach involved 2,841 student records. The data elements involved were student first and last name, student ID, student phone number, school code, student grade, parent email, language indicator and bus route information.
- This information was available to the public for 36 hours, 44 minutes during which time the School Division was able to confirm it was accessed by the following three visitors:

- [Outside Organization]'s bot as it crawled the repository;
- [Outside Organization] IT staff member;
- School Division IT staff member.

[10] My office requested that the School Division clarify the terms of *GitHub code repository*, *personal repository* and *new business repository*:

- *GitHub code repository* is a cloud-based programming tool that allows programming teams to share code in order to better control updates. A Code Repository is a version control system to store programming source code. GitHub used the provider of this code repository in this case. It is like cloud storage but allows granular control over each element in the source code.
- *Personal repository*: GitHub has multiple account types – personal, business and enterprise. The employee working on the project had started it under their personal account as the School Division did not have a business account at the time.
- *New business repository*: The new GitHub account owned by the School Division.

[11] Subsection 28(1) of LA FOIP speaks to disclosure of personal information and provides:

> **28**(1) No local authority shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 29.

[12] In this circumstance, the above specified personal information of 2,841 students and their parents was disclosed without authority and was publicly available for approximately 36 hours.

[13] Therefore, I find a privacy breach occurred.

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

[14] In circumstances where a local authority proactively reports a privacy breach, the focus for my office becomes one of determining whether the local authority appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that the School Division took the privacy breach seriously and appropriately addressed it. In my office's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities*, updated September 2020 (Privacy Breach Guidelines), my office recommends

four best practice steps be taken when a local authority discovers a breach of privacy has occurred starting on page 4. These are:

1. Contain the breach,
2. Notification,
3. Investigate the breach, and
4. Prevent future breaches.

[15] I will now consider if the School Division responded to this matter against these four best practice steps.

Contain the Breach

[16] Page 4 of the Privacy Breach Guidelines discusses what a local authority should consider when containing a breach. It is important to contain the breach immediately, if possible. This means, ensure that personal information is no longer at risk. Containing the breach may involve:

- stopping the unauthorized practice;
- recovering the records
- shutting down the system that was breached;
- revoking access to personal information; and/or
- correcting weaknesses in physical security.

[17] As noted above, the School Division identified that the information was accessed by the following three visitors in the 36 hours, 44 minutes the information was set to public:

- [Outside Organization]'s bot as it crawled the repository;
- [Outside Organization] IT staff member; and
- School Division IT staff member.

[18] My office inquired with the School Division as to how they were able to determine that there were only three visitors and were provided the following explanation:

> GitHub projects have access logs and statistics. Once [School Division] learned of the breach the project was immediately removed from the public share. We also know the usernames of each user that accessed it during the 39 [sic] hours that the data was public and confirmed that two of the users were the [Outside Organization] security team, with

> the final user being the School Division employee working on the project. The first [Outside Organization] access was by the automated software that found the code and the second access was by an [Outside Organization] security employee.

[19] The School Division advised that it requested the Outside Organization destroy any data it received. The Outside Organization provided the School Division with verbal confirmation there was no data to destroy. The Outside Organization advised the School Division it only inspected the data online through its own GitHub account and no data was downloaded or stored in any way.

[20] Further, the Outside Organization advised the School Division that it was its automated system that found the data originally and only reported the finding and it did not capture any data. The Outside Organization security employee only looked at the data.

[21] As GitHub data logs were able to confirm the views of the data and the Outside Organization confirmed there was no data to destroy, I find that the School Division properly contained the breach of privacy.

Notification

[22] The Privacy Breach Guidelines discuss notification starting on page 4. Once the privacy breach is discovered, 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;
- my office;
- the police, if criminal activity is suspected; and/or
- the affected individuals (unless there are compelling reasons why this should not occur.

[23] It is important to note that section 28.1 of LA FOIP requires that, if there is an unauthorized use or disclosure of personal information, the local authority must notify the affected individual(s) if the “incident creates a real risk of significant harm” to the affected individual(s).

[24] Whether or not the local authority determines there is a real risk of significant harm, the best practice is to inform affected individuals and my office of breaches in most cases. Notification should occur as soon as possible after key facts about the breach have been established.

[25] When notifying, it is best to contact the affected individuals directly, such as by telephone, letter or in person. However, there may be circumstances where it is not possible and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on the local authority's website, posted notices such as in public offices, media advisories or advertisements.

[26] A notification should include the following:

- a description of the breach;
- a description of the personal information involved. For example, name, credit card numbers, medical records, financial information, etc.;
- steps taken and planned to mitigate the harm and to prevent future breaches;
- advice on action the individual can take to further mitigate the risk of harm and protect themselves, if necessary. For example, how to contact credit reporting agencies, how to change a health services number or driver's license number, etc.;
- a notice that the individual(s) has the right to complain to my office (include my office's contact information); and
- recognition of the impacts of the breach on the affected individual(s) including an apology.

[27] In its investigation report, the School Division notified employees within the School Division of the breach of privacy. In addition, the School Division notified my office of this matter by proactively reporting it.

[28] The two parents within the School Division were notified of this incident, and one of the parents reported it to the Principal of the school. However, the School Division advised the following in its investigation report:

> Due to the fact that only the [Outside Organization] accessed the information while it was publicly available, and the fact that both affected individuals had been notified, the [School] Division determined that no further notification would be required.

[29] Although the School Division asserts that only the information of two School Division parents was viewed, in this case by their employer (the Outside Organization), the personal information of 2,841 students and their parents were in fact, compromised in this breach of privacy as it was publicly available for over 36 hours. This left the information vulnerable during that timeframe, and the School Division should have taken the necessary steps to notify the students and parents that this breach occurred.

[30] Notifying all affected individuals of the details of this breach, the steps taken to contain the breach and how the School Division responded to mitigate this risk from happening in the future would have been the more appropriate response in this matter.

[31] Therefore, I find that the School Division did not provide appropriate notification of this breach.

[32] I recommend the School Division provide notification of this breach to all affected individuals. Should the School Division follow this recommendation, as the number of affected individuals is large, it may want to advise the affected individuals through notification on its website and the notification can include:

- details of the breach, including containment efforts and steps taken to mitigate the risk of this happening again;
- advise that the breach was proactively reported to my office; and
- a link to this Investigation Report on my office's website.

Investigate the breach

[33] The Privacy Breach Guidelines discuss investigating the breach starting on page 6. Once a breach has been contained, the next step is to investigate the breach. The following are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach?
- What occurred?
- How did the privacy breach occur?
- 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?
- Who are the affected individuals?

[34] The School Division learned of this privacy breach when the Outside Organization's bot was performing an internet crawl for instances of the Outside Organization's information. Through this, it discovered the email addresses of two of its staff on the GitHub repository.

[35] In it's internal investigation, the School Division advised that the following resulted in the privacy breach occurring:

> The web services integration project using this student data was started by an individual employee as requested by management to connect to an automated messaging service called "School Messenger." [School Division] did not currently have a code repository so in the interim while it was being setup, the employee worked on the project from his private persona [sic] code repository. The breach occurred because the privacy settings had not been set appropriately when the new business account was setup, so when the project was transferred from the employees [sic] personal repository the code was exposed until the privacy settings had been changed. When a personal GitHub account is set up, new code defaults to "private" but when a business account is set up, the new code defaults to "public." The employee did not know this at the time the business account was created.

[36] Further, the School Division advised that its IT Manager reviewed the relevant policies and procedures with IT Staff. Upon that review, it concluded that the IT staff was aware of the correct procedure and process for managing private data and confirmed their understanding of the critical importance of data privacy. The School Division further concluded once the policies and procedures were reviewed by the involved staff that the privacy breach occurred due to human error.

[37] Section 23.1 of LA FOIP outlines the explicit duty of a local authority to protect personal information. Section 23.1 of LA FOIP provides:

> **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.

[38] The School Division did not advise my office why the employee did not take the steps necessary to ensure the information was not made publicly available or to ensure the settings were set to private.

[39] By not having the appropriate checks and balances in place to ensure this information would not be publicly available, I find the School Division failed to meet its duty to protect pursuant to section 23.1 of LA FOIP.

[40] Once this privacy breach was discovered, the School Division worked quickly to contain the breach and shut down the unauthorized disclosure – the information was public for approximately 36 hours, was discovered January 29, 2020, and was remedied that same day.

[41] Although it failed to meet its duty to protect, I find the School Division appropriately investigated the breach.

Prevent future breaches

[42] The Privacy Breach Guidelines discuss what a local authority should consider in preventing future breaches similar in nature starting on page 7. Local authorities taking a look at what measures it can take to prevent future breaches is a very important step in responding to a privacy breach. The following are some considerations a local authority can take when considering this step:

- 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?

[43] The School Division advised my office it took the following steps to prevent future breaches related to this incident:

- the School Division purchased the enterprise version of GitHub which allows the content to be made private;
- the IT Manager reviewed privacy policies and procedures with those involved (as outlined above); and
- the IT staff reviewed the procedure for securing data using GitHub and other online services.

[44] Although these are good first steps, the School Division should take further steps to mitigate this risk. The School Division should be thoroughly reviewing these applications prior to using them for its own business purposes.

[45] The Treasury Board of Canada Secretariat has prepared the resource *Government of Canada Cloud Security Risk Management Approach and Procedures* (accessed July 21, 2021 at https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/cloud-security-risk-management-approach-procedures.html#toc3).

[46] This resource, in part, speaks to the importance of a security assessment:

3.6.1 Security Assessment

> When implementing a cloud-based GC [Government of Canada] service, required security controls need to be assessed to establish **<u>the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the business security requirements</u>**. Understanding the overall effectiveness of security control is essential in determining and managing the residual risks….
>
> …
>
> **3.7 Continuous Monitoring and Authorization Maintenance**
>
> The GC cloud risk management approach extends beyond implementation by incorporating activities for continuous monitoring and maintenance of authorizations during the operation phase of cloud-based GC services. Through continuous monitoring, GC consumer organizations have the necessary capabilities to identify security deviations from the authorizations state… **<u>Through authorization maintenance…organizations have the necessary capabilities to react to these deviations in a timely and effective manner</u>**.
>
> [Emphasis added]

[47] It does not appear that the School Division conducted a thorough assessment of the GitHub security settings before it began using the application. In addition, in order to proactively ensure security settings do not change over time, it should continually review security settings and updates to the application (and other applications) to mitigate the risk of a privacy breach in the future.

[48] Although it did advise my office that it has now reviewed the procedure for securing data using GitHub and other online services, the School Division did not provide me any details going forward to mitigate the risk of this happening again with GitHub or any other system.

[49] I find the School Division did not provide my office with enough detail of how it will prevent future breaches of GitHub or similar applications. I recommend the School Division implement a security assessment and ongoing security review process for new and existing applications, including GitHub.

[50] I thank the School Division staff for their cooperation and assistance during this investigation.

III FINDINGS

[51] I find a privacy breach occurred.

[52] I find that the School Division properly contained the breach of privacy.

[53] I find that the School Division did not provide proper notification of this breach.

[54] I find the School Division failed to meet its duty to protect pursuant to section 23.1 of LA FOIP.

[55] I find the School Division appropriately investigated the breach.

[56] I find the School Division did not provide my office with enough detail of how it will prevent future breaches of GitHub or similar applications.

IV RECOMMENDATIONS

[57] I recommend the School Division provide notification of this breach to all affected individuals.

[58] I recommend the School Division implement a security assessment and ongoing security review process for new and existing applications, including GitHub.

Dated at Regina, in the Province of Saskatchewan, this 11th day of August, 2021.

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