

INVESTIGATION REPORT 218-2017

Regina School Division No. 4

December 19, 2017

Summary: Thousands of documents were uploaded to a subdirectory of a church's website by a teacher. Many of the documents contained the personal information of students. A concerned individual discovered the documents and reported it to the Information and Privacy Commissioner (IPC). The IPC undertook an investigation. In the course of the investigation, he found that The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP) did not authorize such a disclosure of personal information. In working with Regina School Division No. 4 (Regina Public Schools), the documents were removed from the subdirectory of the church's website and from the cache of the search engine Google. Furthermore, Regina Public Schools notified the students of this particular teacher of this privacy breach. The IPC made a number of recommendations including notifying students (and their families) who were not the students of the teacher but were still affected by this privacy breach. He also recommended that Regina Public Schools create guidelines for teachers that detail what records they should be keeping, for how long, and how they should be storing the records.

I BACKGROUND

- [1] A teacher at W.F. Ready School, an elementary school in Regina, is the website administrator for a local church. He hosted the church's website from his personal computer. Within a subdirectory of the church's website, he uploaded school-related documents. The documents included teaching material, administrative documents such as letters to parents about field trips, and student information.
- [2] On September 1, 2017 and September 5, 2017, my office was notified by a concerned individual that student information had been uploaded to the subdirectory of the church's

website. He indicated to my office that he was using Google's search engine to look up information. Within the search results was the information on the church's subdirectory containing student information. My office accessed the website and noted there were over 2000 documents that had been uploaded to the subdirectory.

[3] W.F. Ready School is a school within Regina School Division No. 4 (Regina Public Schools). Therefore, on September 5, 2017, my office notified Regina Public Schools that it would be undertaking an investigation.

II DISCUSSION OF THE ISSUES

[4] Regina Public Schools qualifies as a local authority as defined by subsection 2(f)(viii) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

1. Was the information uploaded to the subdirectory of the church's website personal information as defined by section 23 of LA FOIP?

[5] Subsection 23(1) of LA FOIP defines personal information 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, fingerprints or blood type of the individual;

(f) the personal opinions or views of the individual except where they are about another individual;

(g) correspondence sent to a local authority by the individual that is implicitly or explicitly of a private or confidential nature, and replies to the correspondence that would reveal the content of the original correspondence, except where the

correspondence contains the views or opinions of the individual with respect to another individual;

(h) the views or opinions of another individual with respect to the individual;

(i) information that was obtained on a tax return or gathered for the purpose of collecting a tax;

(j) information that describes an individual's finances, assets, liabilities, net worth, bank balance, financial history or activities or credit worthiness; or (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.

[6] As noted in the background, some of the documents that were uploaded to the subdirectory of the church's website included student information. Some examples of the information included students' photographs, grades, passwords, and birth dates. I find that such information qualifies as personal information as defined by subsection 23(1) of LA FOIP.

2. Does the uploading of students' personal information to a subdirectory of a website qualify as a "disclosure" under LA FOIP?

- [7] The term "disclosure" means the sharing of personal information with a separate entity that is not a division or branch of the local authority.
- [8] Uploading the students' personal information to a subdirectory of the church's website means that the personal information was being shared with the public. Therefore, I find that this action qualifies as a disclosure.

3. Did Regina Public Schools have authority to disclose the students' personal information under LA FOIP?

[9] A privacy breach occurs when a local authority collects, uses, and/or discloses personal information that is not in accordance with LA FOIP. In this case, we must determine if Regina Public Schools disclosed personal information in accordance with LA FOIP.

[10] Local authorities must only disclose personal information in accordance with section 28 of LA FOIP. Subsection 28(1) of LA FOIP provides as follows:

28(1) No local authority shall disclose personal information in its possession or 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.

[11] I find that section 28 of LA FOIP did not authorize the disclosure of the students' personal information.

4. Did Regina Public Schools respond appropriately to this privacy breach?

- [12] My office recommends that local authorities take the following five steps when responding to a privacy breach:
 - Contain the breach,
 - Notify affected individuals,
 - Investigate the breach,
 - Prevent future breaches, and
 - Write a privacy breach report.
- [13] I will consider each of these steps to determine if Regina Public Schools adequately responded to the privacy breach.

Contain the breach

- [14] The first step in responding to a privacy breach is containing the breach. This means to recover the personal information or to stop the unauthorized practice when the local authority learns of the breach.
- [15] As noted in the background section of this report, my office notified Regina Public Schools on September 5, 2017 of the situation. Soon after it was notified, Regina Public Schools downloaded the documents from the church's website. Downloading the documents was

important so it could know precisely what information had been uploaded to the subdirectory of the website.

- [16] Then, Regina Public Schools contacted the teacher it believed to have uploaded the documents to the subdirectory of the church's website. The teacher confirmed it was him.
- [17] On September 6, 2017, the teacher confirmed in writing to Regina Public Schools that all the documents had been deleted from his personal computer, the subdirectory on the website, and from a personal flash drive.
- [18] The teacher also voluntarily turned over his personal computer to Regina Public Schools so it can ensure all files were contained.
- [19] Even though the documents had been deleted from the subdirectory of the website, Internet search engines store a cached version of websites and webpages that they index. That is, a snapshot of webpages are taken and stored temporarily within the search engine's cache. In this case, the documents containing students' personal information had been cached by Google. So even though the teacher had removed the documents from the subdirectory of the website, the search engine Google had indexed all the documents and stored it within its cache. Therefore, documents containing students' personal information were still available to the public through Google's cache. Entering search terms into Google's search bar and then clicking on the arrow that appears next to the URL of the search results. An example of the arrow next to a URL is shown below:

Office of the Saskatchewan Information and Privacy Commissioner | IPC https://oipc.sk.ca/

The Saskatchewar Cached d Privacy Commissioner is an independent office of the Saskatchewan Legender bly. It oversees three Saskatchewan ...

Contact Us

Contact Us. Home / Contact Us. Saskatchewan Information and ...

Reports

Use the following tools to search IPC

About IPC

About IPC. Jurisdiction and Mandate. The Saskatchewan ...

The Commissioner About - The Commissioner ... He was

- [20] My office contacted Google Canada for advice on how cached documents could be removed. It gave us advice on how the website administrator could claim control of the website in Google Webmaster tools. Then, the website administrator could use tools within Google Webmaster to have Google's cache refreshed. My office passed on the advice to Regina Public Schools.
- [21] Regina Public Schools used Google Webmaster tools to request Google to re-crawl the church's website so that the documents would not be available to the public from Google's cache. This required a persistent effort by Regina Public Schools as each re-crawling did not always result in the removal of all cached documents. For example, two cached files (that contained personal information) still existed after a re-crawl. Therefore, to remove the contents of the two files, Regina Public Schools took note of the names of the two files. It created two new files containing benign text. The two new files were named the same as the two old files. It then uploaded two new files containing benign text using the same exact directory path of the two old files. It then re-requested Google to re-crawl the church website. This resulted in the two new files (containing benign text) being captured in the cached files and the two old files that had contained students' personal information were removed.
- [22] After multiple requests to Google to re-crawl the church's website (and specifically the subdirectory that had contained students' personal information), Regina Public Schools indicated to my office that the documents containing students' personal information were removed from Google's cache completely by October 14, 2017. Multiple searches of Google's cache conducted by my office show that documents are no longer available to the public.
- [23] I find that Regina Public Schools has made reasonable efforts to contain this privacy breach.

Notify the affected individuals

- [24] Notifying affected individuals of the privacy breach as soon as possible is important so that individuals can determine how they have been impacted. They can also take steps they feel are necessary to protect themselves from harm such as identity theft.
- [25] As mentioned in the background section of the report, thousands of documents were uploaded to the subdirectory of the church's website. In order to focus their efforts in terms of notifying affected individuals, Regina Public Schools obtained a copy of the server logs from the teacher's personal computer (which hosted the church's website). The server logs showed the accesses to the documents on the website from May 31, 2016 (which is the day in which the teacher first uploaded documents to the subdirectory of the church's website) to September 5, 2017 (which is the day in which my office notified Regina Public Schools of the privacy breach). It is important to note that September 5, 2017 was the last day documents were available through the subdirectory of the church's website before the information was removed and the personal computer was turned over to Regina Public Schools.
- [26] The server logs included the Internet protocol (IP) address of the device accessing documents. Therefore, based on the server logs, Regina Public Schools was able to determine that four documents containing personal information had been accessed from IP addresses of devices that did not belong to the teacher himself or was not from a Googlebot that is used to index webpages. In total, Regina Public Schools determined there were 77 students whose personal information may have been accessed by an unknown person.
- [27] To notify the affected individuals, the Deputy Directors contacted the families of the 77 students by telephone to advise them of the privacy breach. This included what Regina Public Schools has done to address the breach, to discuss concerns, and what the student/families can do to protect themselves. 74 families were successfully contacted. It also had two in-person meetings with the families of the affected individuals. For the remaining students/families, Regina Public Schools is continuing its efforts to contact them.

- [28] I find that Regina Public Schools has made reasonable efforts to notify the families of the students whose information may have been accessed. I also applaud its approach to notify the affected individuals by telephone and in-person. This approach made Regina Public Schools available to the individuals to answer questions and address concerns immediately.
- [29] While most of the documents containing student information belonged to past or present students of this particular teacher, and W.F. Ready has already notified them of this privacy breach, I still have concerns about one document that was uploaded to the subdirectory. The document contained the personal information of many of the students at W.F. Ready School (and not just past or present students of the particular teacher). While the server logs referenced at paragraph [26] may not suggest this document was accessed from the church's website, the document could have still been accessed through Google's cache.
- [30] I recommend that Regina Public Schools notify the students and their families whose information appears in this document. This notification should include the following:
 - a description of the breach,
 - a description of the type of personal information that was lost,
 - a description of possible harm that may come from the loss of the personal information including identity theft or fraud,
 - steps that the individual can take to protect himself or herself,
 - steps taken by Regina Public Schools to prevent a similar privacy breach in the future,
 - an apology,
 - the contact information of someone at Regina Public Schools who can answer questions about the privacy breach,
 - the contact information of my office.
- [31] This notification can enable past and present students of W.F. Ready to be aware of the breach and to take action to protect themselves against the harm of having their personal information uploaded to the Internet such as identity theft.

Investigate the breach

- [32] Investigating the privacy breach to identify the root cause is key to understanding what happened and to prevent similar breaches in the future.
- [33] In this case, the root cause of this privacy breach is a combination of a teacher making a mistake and Regina Public Schools lacking sufficient policies, procedures, and training for its employees on how to manage electronic documents.
- [34] In terms of the teacher, he had uploaded the documents to a subdirectory of the church's website, mistakenly believing he would be the only person, as the website administrator, to be able to access the documents. This was so that he could access the documents from anywhere he had Internet access so he could do his work as a teacher more efficiently.
- [35] In terms of record keeping and record retention, my office reviewed the following.
 - Regina Public Schools' Administrative Procedure 365 "Student Records",
 - Regina Public School's Administrative Procedure 405 "Confidentiality",
 - Regina Public School's Administrative Procedure 115 "Computer Network and Internet",
 - Regina Public School's Administrative Procedure 120 "Information Security".
 - Regina Public School's Administrative Procedure 116 "Use of Board-Owned Technology"
 - Regina Public School's Administrative Procedure 127 "Local Authority Freedom of Information and Protection of Privacy".
- [36] I find that the above administrative procedures do not provide explicit and practical guidance to teachers as to how to maintain records. Teachers maintain a wide-range of records, including students' grades/assessments, completed school assignments, the students' parents'/guardians' contact information, and correspondence between themselves and parents/guardians. Based on the above administrative procedures, it is unclear if teachers should be keeping which records, for how long, and how they should be storing the records.
- [37] I recommend that Regina Public Schools create guidelines that detail 1) what records teachers should be keeping, 2) for how long, and 3) how they should be storing the records.

The guidelines should identify for the teachers what records should be kept. For example, Saskatchewan School Board Association's (SSBA) *Records Retention and Disposal Guide for Saskatchewan School Divisions* indicates that certain student records such as students' final marks and final exams must be kept until three years after a student turns 22 years of age. Therefore, guidelines should be created to instruct teachers on how to preserve these records such as providing the original copies of these records to the school division and then delete/destroy any of the copies they (the teachers) have. Other records, such as seating charts to organize classrooms, could be considered transitory and disposed of once the school year is complete. The guidelines should also include instructions as to how to safely destroy records.

- [38] On the school division's computer network, Regina Public Schools advised my office that its employees are able to store records to either a personal drive or to a group share drive. This being the case, Regina Public Schools should take the position that storing student information on teacher's personal computers is prohibited. I recommend that Regina Public Schools create guidelines that indicate the following:
 - teachers are to only store electronic records to the Regina Public Schools computer network,
 - limit what is saved to the Regina Public Schools laptops and other devices to what teachers are currently working on. Records should be moved promptly to the Regina Public School's computer network regularly and deleted from laptops and other devices,
 - prohibit teachers using personal devices to store students' personal information,
 - encourage teachers to only use devices issued by Regina Public Schools.

Prevent the breach

- [39] Preventing future breaches means to implement measures to prevent breaches from occurring.
- [40] Regina Public Schools indicates that it will take the following steps to prevent or minimize the likelihood of a similar privacy breach:

- Require employees to review documentation that states they are to only access information that is necessary for them to do their jobs,
- Require employees to sign a confidentiality agreement that sets out their responsibilities,
- And continue to provide LA FOIP training to its principals and managers through modules. These modules are intended to be shared by principals and managers with their staff.
- [41] I find the above actions are good first steps in preventing similar privacy breaches in the future. To add further to the actions Regina Public Schools will be taking, I recommend that the confidentiality agreement that will be signed by employees have attached a copy of Regina Public Schools' Administrative Procedure 405 on confidentiality and in its guidelines Regina Public Schools clarify is a broader concept than confidentiality. The agreement should state that the employee has read and understood Administrative Procedure 405. Further, I recommend that employees are required to sign the confidentiality agreement annually so employees are reminded of their responsibilities.
- [42] Further, since the concept of privacy is far broader than confidentiality, I also recommend that Regina Public Schools provide LA FOIP training to not only its principals and managers but to all employees annually. This is so that employees are not only reminded of their responsibilities but they are also given an opportunity to ask questions about how to maintain and protect the privacy of their students as new situations arise (for example, as new technologies are introduced into the classroom, teachers may need instruction on how to properly safeguard students' personal information).

III FINDINGS

- [43] I find that such information qualifies as personal information as defined by subsection 23(1) of LA FOIP.
- [44] I find that the uploading of the personal information to the subdirectory of the website qualifies as a disclosure.

- [45] I find that section 28 of LA FOIP did not authorize the disclosure of the students' personal information.
- [46] I find that Regina Public Schools has made reasonable efforts to contain this privacy breach.
- [47] I find that Regina Public Schools has made reasonable efforts to notify the families of the students whose information may have been accessed.
- [48] I find that Regina Public Schools' administrative procedures do not provide explicit and practical guidance to teachers as to how to maintain records.
- [49] I find that Regina Public Schools is taking good first steps that will prevent similar privacy breaches in the future.

IV RECOMMENDATIONS

- [50] I recommend that Regina Public Schools notify the students and their families whose information appears in the document, as described at paragraph [30].
- [51] I recommend that Regina Public Schools create guidelines that detail 1) what records teachers should be keeping, 2) for how long, and 3) how they should be storing the records as described at paragraph [37].
- [52] I recommend that Regina Public Schools create guidelines that indicate the following:
 - teachers are to only store electronic records to the Regina Public Schools computer network,
 - limit what is saved to the Regina Public Schools laptops and other devices to what teachers are currently working on. Records should be moved promptly to the Regina Public School's computer network regularly and deleted from laptops and other devices,
 - prohibit teachers using personal devices to store students' personal information,
 - encourage teachers to only use devices issued by Regina Public Schools.

- [53] I recommend that the confidentiality agreement that will be signed by employees have attached a copy of Regina Public Schools' Administrative Procedure 405 on confidentiality and in its guidelines Regina Public Schools clarify is a broader concept than confidentiality. The agreement should state that the employee has read and understood Administrative Procedure 405.
- [54] I recommend that employees are required to sign the confidentiality agreement annually.
- [55] I recommend that Regina Public Schools provide LA FOIP training to not only its principals and managers but to all employees annually.

Dated at Regina, in the Province of Saskatchewan, this 19th day of December, 2017.

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