Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 234-2021

Rural Municipality of Pleasantdale No. 398

September 15, 2022

Summary: The Rural Municipality of Pleasantdale No. 398 (RM) received a complaint alleging that the RM inappropriately disclosed the Complainant's personal information. The RM responded to the Complainant agreeing that a privacy breach had occurred due to a human error. The Complainant was not satisfied with the RM's response and asked the Commissioner to investigate. The Commissioner found that a privacy breach occurred as the disclosure was unauthorized. The Commissioner also found that the RM did not manage the privacy complaint appropriately. The Commissioner recommended that the RM develop a privacy policy that is compliant with its duty to protect personal information pursuant to section 23.1 of LA FOIP and ensure that this policy includes steps to handle a privacy breach appropriately. The Commissioner also recommended that if it has not already, the RM request the record back or ensure that the record is destroyed by the other ratepayer. In addition, the Commissioner recommended that the RM ensure its staff and councillors receive privacy training within three months of issuance of this Investigation Report. Finally, the Commissioner recommended that the RM issue an apology letter to the Complainant.

I BACKGROUND

[1] On August 25, 2021, the Complainant contacted the Rural Municipality of Pleasantdale No. 398 (RM) complaining that the RM had disclosed their personal information to another ratepayer. The RM had provided the individual with a copy of a letter that was addressed to the Complainant.

[2] On September 13, 2021, the RM responded to the Complainant. The RM's letter did not discuss its investigation or provide the Complainant with an appropriate response to their privacy concerns.

[3] On September 22, 2021, the Complainant requested that our office investigate this matter.

[4] On September 23, 2021, my office contacted the RM and requested that it complete its investigation pursuant to *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), and that it provide a response to the Complainant by October 7, 2021.

[5] On September 24, 2021, the RM responded to the Complainant and to my office asserting that it had not considered the Complainant's correspondence of August 25, 2021 as a privacy complaint. The RM acknowledged that it mistakenly provided the letter addressed to the Complainant, to the other ratepayer.

[6] On September 27, 2021, the Complainant informed my office that they were still not satisfied with the RM's response and requested that my office investigate this matter.

[7] On September 29, 2021, my office notified the RM and the Complainant of my office's intention to undertake an investigation. My office requested a copy of the RM's internal investigation report regarding this matter. My office also invited the Complainant to provide any further details regarding the alleged breach of privacy.

[8] On October 1, 2021, the RM provided is internal investigation report to my office. The Complainant did not provide any further information to my office.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[9] The RM qualifies as a "local authority" pursuant to section 2(f)(i) of LA FOIP. Therefore, I have jurisdiction to conduct this investigation.

2. Did a privacy breach occur?

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

[11] Along with its internal investigation report to my office, the RM provided a copy of the letter that it had provided to another ratepayer by mistake. My office noticed that the letter contains the Complainant's name and mailing address.

[12] The RM did not cite any part of section 23(1) of LA FOIP in this matter. I note that the data elements listed above would qualify as personal information as defined by sections 23(1)(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:
>
> …
> (e) the home or business address, home or business telephone number or fingerprints of the individual;
> …
>
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
> …

[13] Therefore, I find that the Complainant's personal information is involved pursuant to sections 23(1)(e) and (k)(i) of LA FOIP. As such, LA FOIP is engaged and the privacy rules outlined in Part IV of LA FOIP will guide this investigation.

[14] In this matter, I have established that the RM provided a copy of a letter containing the Complainant's personal information to another ratepayer. The other ratepayer contacted the Complainant to tell them what had occurred. The Complainant stated that they then filed a privacy compliant with the RM on July 7, 2021.

[15] In its internal investigation report, the RM stated that it did not receive a complaint from the Complainant on July 7, 2021. The RM asserted that it received an email from the Complainant on August 25, 2021, and responded to them on September 13, 2021, by letter. The RM stated that it did not view the Complainant's email dated August 25, 2021 as a privacy complaint. My office noted, though, that the Complainant's email dated August 25, 2021, clearly stated in part:

> …I still want to know why the letter that the Administrator sent to me dated June 11, 2021 was given out to other ratepayers in the Municipality. This letter was addressed to me and contained my personal information…

[16] Upon reading the RM's response letter dated September 13, 2021, my office noted the RM cited section 28(1) of LA FOIP, but did not explain to the Complainant if it had conducted an internal investigation, or if it believed a privacy breach had occurred. The RM also did not discuss the four best practice steps my office advises to address a privacy breach.

[17] On September 23, 2021, my office contacted the RM and requested that it complete its internal investigation pursuant to LA FOIP and provide a response to the Complainant by October 7, 2021. By conducting a privacy breach investigation, a local authority can assess its authority to collect, use and/or disclose personal information. If a local authority cannot establish authority, then a privacy breach has occurred.

[18] In this matter, the RM provided the Complainant's personal information to someone who is not affiliated with the RM, such as an employee or councillor. In my office's Investigation Report F-2014-002 at paragraph [53], it was stated that to "disclose" means to share personal information with a separate entity that is not a division or branch of a

local authority that has possession or control of that record or information. Therefore, in this matter, we are looking at a disclosure.

[19] Section 28(1) of LA FOIP establishes that local authorities, which includes the employees of the local authority, can only disclose personal information in its possession or under its control with the consent of the individual. To disclose an individual's personal information without consent, the local authority must have authority pursuant to sections 28(2) and 29 of LA FOIP. Section 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.

[20] In this case, the Complainant clearly did not provide their consent. As well, it is not clear to me if any part of section 28(2) of LA FOIP would apply in this case, and section 29 of LA FOIP would have no application. The RM also did not state in its investigation report if it had any authority to disclose the Complainant's personal information. As such, I find that the disclosure was unauthorized and that a privacy breach occurred.

3. Did the RM respond appropriately to the privacy breach?

[21] At this stage, my office then moves onto considering how a local authority managed the privacy breach. According to my office's *Rules of Procedure*, my office will analyze whether the public body properly managed the breach and took the following steps in responding to the privacy breach:

- Contained the breach (as soon as possible);
- Notified affected individuals (as soon as possible);
- Investigated the breach; and
- Prevented future breaches.

[22] Based on the information the RM provided to my office, I will now assess how it addressed each of these four steps. I will make any recommendations, as necessary, following my analysis of each of the four steps.

Contained the breach (as soon as possible)

[23] 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

(Privacy Breach Guidelines for Government Institutions and Local Authorities (*Privacy Breach Guidelines*), updated August 2022, page 4)

[24] In its internal investigation report, the RM did not provide evidence to support if it took any action to get the letter in question back from the other ratepayer, or if it asked that ratepayer to shred or destroy the letter. The RM simply repeated multiple times, that it did not know a privacy breach had occurred until September 23, 2021, when my office contacted it.

[25] Based on the RM's response, I find that there was no containment.

[26] If it has not already, I recommend that the RM should request the record back or ensure that the record is destroyed by the other ratepayer.

Notified affected individuals (as soon as possible)

[27] Notification to individuals affected by the breach should occur as soon as possible after key facts about the breach have been established. It is best to contact 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 a website, posted notices, media advisories and advertisements. Ensure the breach is not compounded when using indirect notification. Notifications 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 them as a result of the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies).
- Contact information of an individual within your organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

(*Privacy Breach Guidelines*, pp. 4-6)

[28] In its internal investigation report to my office, the RM explained that it mistakenly attached the letter in question to the other ratepayer's package, because it was on the same workspace. The RM asserted that as it did not know a privacy breach had occurred until September 23, 2021; therefore, it did not provide any notification to the Complainant.

Going forward, once the RM identifies a privacy breach, it should consider providing notification to any affected individuals.

[29] Based on the RM's response, I find that there was no notification.

Investigated the breach

[30] Once a breach has been contained the next step is to investigate the breach. Here 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?

(*Privacy Breach Guidelines*, pp. 6-7)

[31] As stated previously in this Investigation Report, the RM stated it was not aware it had breached the Complainant's privacy until my office contacted it on September 23, 2021. At that point, it had not conducted an investigation.

[32] In response to my office's request to complete the *Privacy Breach Investigation Questionnaire*, the RM's administrator stated that they made a mistake, as the papers got mixed up on their workspace. They also added that they do everything they can to ensure that personal information is not disclosed to ratepayers. So, the question is what do they do? The RM did not provide any evidence to explain the safeguards it has in place, if any.

The RM did not identify the root cause of this privacy breach, which appears to be human error due to a lack of administrative and physical safeguards.

[33] Pursuant to section 23.1 of LA FOIP the RM has a duty to protect personal information of its citizens. Section 23.1(a) of LA FOIP 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;

[34] Administrative safeguards are 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 (IMSPs), auditing programs, records retention and destruction schedules, and access restrictions (*Privacy Breach Guidelines*, p. 2).

[35] Physical safeguards are physical measures, policies, and procedures to protect personal information and related buildings and equipment from unauthorized intrusion and natural and environmental hazards. Examples include locked filing cabinets, offices and storage rooms, alarm systems, and clean desk approaches (*Privacy Breach Guidelines*, p. 2).

[36] In this case, the RM did not identify if any of these were issues, but admitted it made an error by mixing up the letters. The RM should consider developing procedures for its administrative staff to manage the RM's day-to-day operations and maintain a clean desk policy to avoid an unorganized workspace. For example – if the RM is mailing out multiple letters or packages on a day, staff should take the time to ensure the name on the mailing label, the letter and the package all match.

[37] Based on the RM's response, I find that the RM did not conduct a thorough investigation.

[38] I recommend that the RM develop a policy and procedure that includes steps to handle a privacy breach appropriately.

Prevented future breaches

[39] 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?

(*Privacy Breach Guidelines*, pp. 7-8)

[40] In its internal investigation report, the RM asserted that it had policies and internal guides to ensure that personal information of ratepayers was not disclosed. The RM provided a copy of its policies and internal guidelines for my office to review and confirmed that it was the only "formal policy that the municipality has at the moment…"

[41] Upon review of the RM's policy and procedures, I note that this policy did not have any privacy component listed. There are no definitions regarding personal information, or information on collection, use or disclosure. Further there is no mention of the RM's duty to protect the personal information that it has in its possession or under its control. My office also noted that the RM's staff, including the Administrator involved in this incident, had not received any privacy training.

[42] Based on the RM's response, I find that there are no measures in place to prevent any future breaches.

[43] I recommend that the RM develop a privacy policy, that is compliant with its duty to protect personal information pursuant to section 23.1 of LA FOIP. I also recommend that the RM provide privacy training to its staff and councillors within three months of issuance of this Investigation Report.

[44] Finally, I recommend that the RM issue an apology to the Complainant.

III FINDINGS

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

[46] I find that the Complainant's personal information is involved pursuant to sections 23(1)(e) and (k)(i) of LA FOIP.

[47] I find that a privacy breach occurred.

[48] I find that the RM did not contain the privacy breach.

[49] I find that the RM did not notify the affected individual.

[50] I find that the RM did not thoroughly investigate the privacy breach.

[51] I find that the RM did not have any measures in place to prevent any future privacy breach.

IV RECOMMENDATIONS

[52] I recommend that the RM develop a privacy policy that is compliant with its duty to protect personal information pursuant to section 23.1 of LA FOIP and ensure that this policy includes steps to handle a privacy breach appropriately.

[53] I recommend that if it has not already, the RM request the record back or ensure that the record is destroyed by the other ratepayer.

[54] I recommend that the RM provide its staff and councillors with privacy training within three months of issuance of this Investigation report.

[55] I recommend that the RM issue an apology to the Complainant.

Dated at Regina, in the Province of Saskatchewan, this 15th day of September, 2022.

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