Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 166-2021

Rural Municipality of North Qu'Appelle No. 187

March 29, 2022

Summary: The Organized Hamlet of Pasqua Lake Board, within the Rural Municipality of North Qu'Appelle No. 187 (RM), sent an email to a number of individuals and did not use the blind carbon copy field for the email addresses. The Organized Hamlet of Pasqua Lake Board notified all recipients of the breach and requested they delete the email. The Complainant was one of the email recipients and submitted a privacy breach complaint to the RM. The RM responded to the Complainant advising the privacy breach had been appropriately responded to and the file was closed. The Complainant was dissatisfied with the response and requested my office undertake a privacy breach investigation. My office undertook an investigation into the RM's actions to respond to the privacy breach. The Commissioner found that the RM did not take appropriate action in response to the privacy breach and made a number of recommendations to the RM to ensure appropriate policy or procedures were in place, as well as implementation of appropriate safeguards to protect personal information.

I BACKGROUND

[1] On April 20, 2021, the Complainant submitted a privacy complaint to the Rural Municipality of North Qu'Appelle No. 187 (RM) as follows:

> On April 9 2021 8:01 am our Hamlet Chair [name of the Chair of the Organized Hamlet of Pasqua Lake Board] mailed out some information to the rate payers of Pasqua Lake and leaked out everyone's email addresses to everyone on that list (well over 200 email addresses).
>
> On April 9 2021 at 11:19 am we received an apology,
>
> "I need to send out my deepest apology to all the recipients of the ohpl gmail grouping for my screw up in my earlier email today. In my rush I failed to address the email via

> bcc and unfortunately everyone's email address can be viewed, which should never have happened. It is my hope that everyone will respect each other's right to privacy and not to use for nefarious purposes. PLEASE DELETE THE EMAIL IMMEDIATELY.
>
> Again my deepest regrets.
>
> [name of the Chair of the Board of the Organized Hamlet of Pasqua Lake]
> OHPL Chair"
>
> I waited for the RM meeting on April 13 2021 to see if it would be mentioned and nothing, I waited for the Hamlet meeting on April 20 2021 again nothing was mentioned about this serious offence.
>
> To me this is a huge breach in trust and an invasion of privacy and nothing was said, mentioned or done on the RM or Hamlet level.
> …

[2] On May 3, 2021, the RM responded to the Complainant stating:

> This letter is a follow up in response to your complaint regarding the release of personal email addresses by the Chair of the Pasqua Lake Hamlet Board. As noted on April 9th, 2021 at approximately 8:01 a.m., the Hamlet Chair, [name of the Chair of the Organized Hamlet of Pasqua Lake Board], sent our a notice under the Hamlet's Gmail account which included all email addresses for that particular group.
>
> On April 26, 2021, a review of the complaint and process was carried out. In accordance with the requirements of the Office of the Saskatchewan Information and Privacy Commissioner, the following steps are to be taken when a privacy breach occurs –
>
> 1. Contain the breach as soon as possible.
> 2. Notify the affected individuals at first reasonable opportunity.
> 3. Investigate the situation
> 4. Prevent.
>
> Upon reviewing the events of April 9th with [name of the Chair of the Organized Hamlet of Pasqua Lake Board], the following was identified. As stated above, the release of emails occurred at approximately 8:01 a.m. Upon realizing the situation, [name of the Chair of the Organized Hamlet of Pasqua Lake Board] sent out a follow up email on April 9th at 11:19 a.m… apologizing for the action; explaining the reason why it occurred and asking affected parties to respect others right to privacy and not sue for nefarious purposes (quote). Also in [name of the Chair of the Organized Hamlet of Pasqua Lake Board]'s follow up email, he clearly states those receiving the email to "delete the email immediately".
> [Name of the Chair of the Organized Hamlet of Pasqua Lake Board]'s actions regarding the follow up email would relate to Steps 1 and 2, "Contain and Notify", as outlined by

> the Privacy Commissioners Office. The review conducted on April 26, relates to Step 3, "Investigate". With respect to Step 4, "Prevent", [name of the Chair of the Organized Hamlet of Pasqua Lake Board]'s actions at the time were not intentional, nor malicious in nature and appear to be an unfortunate mistake.
>
> [Name of the Chair of the Organized Hamlet of Pasqua Lake Board] is remorseful in the realization of his actions that, in his haste to sent out the email, he made this error and he stated that he will take the time necessary to ensure that any future communication will include the Blind Copy (Bcc) component for recipients to ensure this situation does not re-occur.
>
> R.M. 187 of North Qu'Appelle feels this matter has been dealt with and is closed. If you wish to pursue this issue further, you can contact the Office of the Privacy Commissioner or the Provincial Ombudsman.

[3] On July 13, 2021, my office notified the Complainant and the RM that my office would be investigating the matter.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[4] As noted above, the Chair of the Organized Hamlet of Pasqua Lake Board sent an email to a number of individuals and did not use the blind carbon copy filed for the email addresses. After sending the email, the Chair of Organized Hamlet of Pasqua Lake Board apologized for the oversight and requested all recipients delete the email. The Complainant, one of the email recipients, had concerns with this incident and contacted the RM to submit a privacy breach complaint. The RM responded advising the breach had been appropriately responded to. I will first address which body qualifies as a local authority under *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

[5] Section 2(f)(i) of LA FOIP provides that a municipality qualifies as a local authority. *The Municipalities Act* defines a municipality at section 2(1)(w) as "a town, village, resort village, rural municipality or restructure municipality." Section 2(1)(rr) of *The Municipalities Act* provides that rural municipality "means a rural municipality incorporated or continued pursuant to this Act." Organized Hamlet is defined at section

2(1)(x) of *The Municipalities Act* as "an area declared to be an organized hamlet by order of the minister pursuant to this Act or any former Act providing for the establishment of organized hamlets."

[6] Further, sections 49(3) and 51(1) of *The Municipalities Act* provides:

> **49**(3) Notwithstanding any other provision of this Act, at the request of a hamlet board, the minister may designate an organized hamlet with a population in excess of 100 as a separate division within the rural municipality in which the organized hamlet is located, to be represented by its own councillor.
> …
>
> **51**(1) Subject to subsections (2) and (3), the persons within an organized hamlet may apply to the minister, in accordance with the procedures set out in Division 2 for the incorporation of the organized hamlet as a resort village or village.

[7] The Government of Saskatchewan's website provides the following regarding organized hamlets:

> Organized hamlets (OH) are designated by Minister's order, have a legal boundary and are also governed by a RM. The residents of an OH elect a three-person advisory board to represent the community to the RM council. The RM is the legal governing body.
>
> https://www.saskatchewan.ca/government/municipal-administration/community-planning-land-use-and-development/municipal-status-and-boundary-changes/establishing-an-organized-hamlets

[8] The Organized Hamlet of Pasqua Lake is an Organized Hamlet within the RM. The RM is a municipality, and therefore is a local authority pursuant to section 2(f)(i) of LA FOIP. Therefore, I have jurisdiction to investigate this matter.

[9] The RM, as the body that qualifies as a local authority, is responsible to ensure all RM staff, members of the RM council and members of its Organized Hamlet boards are compliant with LA FOIP.

2. Is personal information involved and is LA FOIP engaged?

[10] In order for LA FOIP to be engaged in a privacy breach investigation, there must be personal information, as defined by section 23(1) of LA FOIP, involved. Section 23(1) of LAFOIP provides:

> **23**(1) Subject to subsections (1.1) and (2), "personal information" means personal information about an identifiable individual that is recorded in any form…

[11] The list provided at subsection 23(1) of LA FOIP is not exhaustive; there are other types of information that may not be listed, but still considered personal information. To be personal information, I must consider if: 1) there is an identifiable individual; and 2) if the information is personal in nature. The definitions of each are as follows:

- Identifiable means it must be reasonable to expect that an individual may be identified if the information were disclosed.
- Personal in nature means that it reveals something about the individual.

[12] In my office's Investigation Report 212-2019, my office discussed if personal email addresses were considered to be personal information:

> [8] The email contains the Complainant's first letter of their first name and complete last name and is their personal email address. This is also the case for the other individuals, in this matter, whose personal (non-business-related) email addresses containing either their partial or full name were also disclosed by the City, as well as why the email was being sent.
>
> [9] In Investigation Report 230-2017, 237-2017, 238-2017, 240-2017 regarding Good Spirit School Division, I considered a matter whereby a principal disclosed the list of all approved substitute teachers to another substitute teacher. In that matter, I found that the combination of information, which included data elements of first and last name, email address and notes about some of the teachers, qualified as personal information pursuant to subsection 23(1) of LA FOIP. Similarly, I find that personal information is involved in this matter.
>
> [10] As the City has not disputed that a breach occurred, my next step is to review how the City managed the breach.

[13] As was the case in the investigation involving the City of Regina, the RM has not disputed that the information at issue qualifies as personal information and that a breach occurred. Therefore, I find that personal information is involved and that LA FOIP is engaged.

[14] In the next section of the Report, I will consider the actions taken by the RM to respond to the privacy breach.

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

[15] In my office's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities*, updated September 2021 (*Privacy Breach Guidelines*), I recommend four best practice steps in responding to a privacy breach:

- Contain the privacy breach
- Notification
- Investigate the breach
- Prevent future breaches.

(Privacy Breach Guidelines, pp. 4-7)

[16] I will use these steps to assess the RM's response to the breach.

Contain the breach

[17] Soon after a local authority learns of a privacy breach, it should contain and recover any personal information/personal health information that is involved. This will require determining how broad the privacy breach is and what type of records are involved.

[18] On the same day, after realizing the error, the head of the Board of the Organized Hamlet of Pasqua Lake sent an email to all those that had received the email requesting they delete the email. It does not appear that there was a request for the individuals to confirm the email had been deleted, as such, it is not clear if this breach has been fully contained.

[19] While steps were taken to contain the breach in a timely manner, in the future the RM, may want to consider what other actions could be taken. This may include attempting to recall the email and/or requesting recipients respond confirming the email has been deleted.

[20] I find that the RM has not fully contained the privacy breach.

Notify affected individuals

[21] Notice to affected individuals should happen as soon as possible when learning of a breach. Notifying an individual that their personal information has been inappropriately accessed or disclosed is important for a number of reasons. Not only do individuals have a right to know, they need to know in order to protect themselves from potential harm that may result from the inappropriate disclosure. Unless there is compelling reason not to, local authorities should always provide notification.

[22] The Chair of the Board of the Organized Hamlet of Pasqua Lake sent an email to all recipients advising of the error. However, there are other elements that the RM should ensure are in notifications to affected individuals. My office's *Privacy Breach Guidelines* suggests the following elements be included in notification to affected individuals:

> 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, how to change a health services number or driver's license number etc.);
> - 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); and
> - recognition of the impacts of the breach on affected individuals and, an apology.

[23] Public bodies should also consider proactively reporting privacy breaches to my office. This means that when a public body learns of a breach, it reports the incident to my office. While proactively reporting is not mandatory, my office does encourage public bodies to proactively report. If my office determines the breach has been responded to appropriately, there may be an opportunity to informally resolve the matter, rather than issuing a public

report on the matter. Some advantages of proactively reporting are discussed in my office's *Privacy Breach Guidelines*:

> Some of the benefits of proactively reporting include:
>
> - may reduce the need for the IPC to issue a report on the matter;
> - receive timely, expert advice from the IPC: the IPC can help guide the public body on what to consider, what questions to ask and what parts of the legislation may be applicable;
> - should the media get wind of the privacy breach, the public body can assure the public that it is working with the IPC to address the matter; and
> - should affected individuals contact the IPC, we can assure the individuals that we are working with your organization.

[24] I find that the RM notification to the affected individuals did not include all of the recommended elements for a notification.

Investigate the breach

[25] Investigating the privacy breach to identify the root cause is key to understanding what happened. Identifying the root cause will help prevent similar breaches in the future. The internal investigation should also consider whether the safeguards that were in place at the time of the incident were adequate.

[26] The RM's response to my office's notification that we would be undertaking an investigation indicates that the breach occurred due to human error. Its response did not address what safeguards were in place at the time of the incident. My office followed up with the RM to inquire if the RM had a privacy policy or email policy in place. As well, my office inquired if the RM or the Organized Hamlet of Pasqua Lake conducts privacy training for its staff and council/board. The RM responded on February 24, 2022, advising the RM does not have a privacy policy. It also advised that neither the RM Council nor the Organized Hamlet Boards have received any privacy training, however the Administrator and Assistant Administrator had taken part in some past workshops and seminars put on by the Saskatchewan Rural Municipal Administrators Association. The RM did advise that the Organized Hamlet of Pasqua Lake had a communications policy. The RM provided my

office with a copy of this policy. However, in reviewing this policy, it discusses that electronic communications will be sent to individuals that have provided email addresses. It does not address risks and safeguards for the electronic communication of personal information.

[27] Section 23.1 of LA FOIP provides the following regarding the duty to protect:

> **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.

[28] My office's *Privacy Breach Guidelines* provides the following regarding the duty to protect personal information:

> FOIP, LA FOIP, and their Regulations provide reasons a public body should collect, use, and disclose personal information. Any collections, uses, or disclosures unauthorized by FOIP or LA FOIP would be a privacy breach. Additionally, FOIP and LA FOIP each include an explicit duty on public bodies to protect personal information (see sections 24.1 of FOIP and 23.1 of LA FOIP).
>
> Sections 24.1 of FOIP and 23.1 of LA FOIP require that a public body have administrative, technical and physical safeguards to protect personal information.
>
> *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.

> *Technical safeguards* are the technology and the policy and procedures for its use that protect personal information and control access to it. Examples include separate user identifications, passwords, firewalls, identification and authentication controls, virus scanners, and audit capabilities in digital systems.
>
> *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.
>
> Sections 24.1(a) of FOIP and 23.1(a) of LA FOIP indicate that a public body must protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control.
> …
>
> *Confidentiality* implies a trust relationship between the person supplying information and the individual or organization collecting or using it.
> Sections 24.1(b) of FOIP and 23.1(b) of LA FOIP indicate that public bodies must protect against any reasonably anticipated:
>
> - threat or hazard to the security or integrity of the personal information in its possession or under its control;
> - loss of the personal information in its possession or under its control; and/or
> - unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control.
>
> *Threat* means a sign or cause of possible harm.
> *Hazard* means a risk, peril, or danger.
>
> *Security* means a condition of safety or freedom from fear or danger.
> …
>
> Unauthorized disclosure refers to the act of revealing, showing, providing copies, selling, giving, or relaying the content of personal information in ways that are not permitted under sections, 29 or 30 of FOIP (sections 28 or 29 of LA FOIP).
>
> Sections 24.1(c) of FOIP and 23.1(c) of LA FOIP indicate that public bodies should have education programs in place for their employees which address the public body's duties under FOIP/LA FOIP, safeguards the public body has established, the need-to-know, and consequences for violating FOIP/LA FOIP. The Office of the Information and Privacy Commissioner (IPC) has indicated that annual training is best practice.

[29] The only safeguard that was in place was a communication policy that did not address the RM's privacy obligations when using electronic communications. I find that the RM did

not have appropriate safeguards in place at the time of the privacy breach to meet its duty to protect personal information pursuant to section 23.1 of LA FOIP.

[30] I recommend the RM develop and implement a policy or procedure for responding to privacy breaches. This should include measures to contain a privacy breach, what parties should be notified of the privacy breach, and the elements to include in notification to affected individuals. As well, it should include what steps to take to investigate a privacy breach and consideration of preventative measures. The policy or procedures should also identify who the Privacy Officer is for the RM and direct the RM staff, members of the RM council and members of its Organized Hamlet boards to report privacy breach incidents to the Privacy Officer.

[31] I recommend the RM develop and implement a privacy policy that addresses collection, use, disclosure and safeguarding of personal information to ensure it meets its obligations under LA FOIP.

[32] I recommend the RM develop and implement a confidentiality agreement to be signed annually by all RM staff, members of the RM council and members of its Organized Hamlet boards.

[33] I recommend the RM implement annual access and privacy training for all RM staff, members of the RM council and members of its Organized Hamlet boards.

Plan for prevention

[34] Local authorities should be safeguarding personal information. Administrative, physical and technical safeguards should be reviewed regularly to determine their adequacy in protecting information, including after the discovery of a privacy breach.

[35] As noted in the previous section of this Report, section 23.1 of LA FOIP provides the following regarding the duty to protect personal information by implementing appropriate safeguards. However, in this incident, I found that the RM did not have appropriate

safeguards in place. The RM indicated that, in the future, additional time would be taken to ensure email addresses were entered in the blind carbon copy (bcc) field to prevent future occurrences. The RM has taken corrective action to address this incident and I agree that taking additional time to ensure information is entered in the bcc field can assist with reducing errors. However, there are additional safeguards that the RM can implement to prevent future privacy breaches.

[36] I find that the RM has not implemented sufficient safeguards to prevent future occurrences of privacy breaches.

[37] In my office's Investigation Report 212-2019, my office investigated a privacy breach incident involving a similar incident where email addresses were not entered into the bcc field. In that report, the Commissioner recommended the following:

> [23] In its investigation report, the City stated its plan for prevention was to "[e]nsure procedures indicate use of bcc for group and email messaging". It appears, however, that the City has not added this to its procedures, although it stated, "we touch on that caution [using bcc] in privacy training and will be reinforcing the practice in future training". Providing this caution in training is a good step, and while I find that the City's plan for prevention was adequate, I recommend that the City follow-up on its initial goal of including the use of "bcc" in its written procedures, and implement safeguards, such as ensuring the "bcc" line shows up by default when sending an email, to prevent the same type of breach from occurring again in the future.

[38] The RM should implement similar measures. I also recommend the RM amend its communication policy, or develop and implement a policy for electronic communication, that addresses the use of the bcc field in emails to multiple personal email addresses and addresses the RM's obligations under LA FOIP for the safeguarding of personal information when using electronic communication. These measures should apply to RM staff, members of the RM council and members of its Organized Hamlet boards to reduce the likelihood of this error occurring again in the future.

III FINDINGS

[39] I find that I have jurisdiction to investigate this matter.

[40] I find that personal information is involved and that LA FOIP is engaged.

[41] I find that the RM has not fully contained the privacy breach.

[42] I find that the RM's notification to the affected individuals did not include all of the recommended elements for a notification.

[43] I find that the RM did not have appropriate safeguards in place at the time of the privacy breach to meet its duty to protect personal information pursuant to section 23.1 of LA FOIP.

[44] I find that the RM has not implemented sufficient safeguards to prevent future occurrences of privacy breaches.

IV RECOMMENDATIONS

[45] I recommend the RM develop and implement a policy or procedure for responding to privacy breaches. This should include measures to contain a privacy breach, what parties should be notified of the privacy breach, and the elements to include in notification to affected individuals. As well as steps to take to investigate a privacy breach and consideration of preventative measures. The policy or procedures should also identify who the Privacy Officer is for the RM and direct the RM staff, members of the RM council and members of its Organized Hamlet boards to report privacy breach incidents to the Privacy Officer.

[46] I recommend the RM develop and implement a privacy policy that addresses collection, use, disclosure and safeguarding of personal information to ensure it meets its obligations under LA FOIP.

[47] I recommend the RM develop and implement a confidentiality agreement to be signed annually by all RM staff, members of the RM council and members of its Organized Hamlet boards.

[48] I recommend the RM implement an annual access and privacy training program for all RM staff, the members of the RM council and the members of its Organized Hamlet boards.

[49] I recommend the RM should explore if its email system can be configured to ensure the bcc field is visible by default when sending an email.

[50] I recommend the RM amend its communication policy, or develop and implement a policy for electronic communication, that addresses the use of the bcc field in emails to multiple personal email addresses and addresses the RM's obligations under LA FOIP for the safeguarding of personal information when using electronic communication. These measures should apply to the RM staff, members of the RM council and members of its Organized Hamlet boards to reduce the likelihood of this error occurring again in the future.

Dated at Regina, in the Province of Saskatchewan, this 29th day of March, 2022.

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