Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 250-2021

Resort Village of Kivimaa – Moonlight Bay

September 6, 2022

Summary: The Resort Village of Kivimaa – Moonlight Bay (Village) breached the privacy of one its ratepayers, the Complainant. The Complainant asked the Commissioner to investigate the matter. The Commissioner found that the Village did not take adequate steps to contain the breach, notify the Complainant, investigate the breach, and did not have an adequate plan for prevention. The Commissioner recommended the Village review its bylaws to ensure they address its obligations regarding how to manage personal information, and that it provide its staff, mayor and councillors with training on *The Local Authority Freedom of Information and Protection of Privacy Act*.

I BACKGROUND

[1] In a letter dated August 20, 2021, an administrator with the Resort Village of Kivimaa-Moonlight Bay (Village) expressed their discontent with the Complainant. The letter outlined issues they had with the Complainant's behaviour and criticism of them, the mayor and Village council. The administrator felt the Complainant was making a "deliberate attempt to demoralize and intimidate", and so wanted to express their frustration at what they felt was ongoing harassment and bullying by the Complainant.

[2] On August 21, 2021, the mayor read the administrator's letter at a public meeting and then instructed the administrator to post it on the Village's website, which the administrator did the same day. The Village confirmed that it left the letter publicly available on its website until September 7, 2021. At the meeting, the mayor also read aloud another letter written by the previous mayor to the Complainant.

[3] On October 9, 2021, the Complainant emailed my office requesting an investigation into the matter.

[4] On October 26, 2021, my office notified both the Village and the Complainant of my office's intention to undertake an investigation.

[5] The Applicant provided their submission to my office on November 15, 2021, and the Village provided its submission to my office on November 24, 2021.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] The Village is a "local authority" pursuant to section 2(f)(i) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP); therefore, I have jurisdiction to conduct this investigation.

2. Did the Village respond appropriately to the privacy breach?

[7] A privacy breach occurs when "personal information" is collected, used, and/or disclosed without authority under LA FOIP. Therefore, to determine if a privacy breach occurred, I need to determine if this matter involves personal information. If so, then I need to determine if there was or was not authority under LA FOIP for the Village to collect, use, and/or disclose the personal information.

[8] What qualifies as personal information is enumerated at section 23(1) of LA FOIP, although the list is not exhaustive. To determine if personal information is involved, a public body needs to assess if: 1) there is an identifiable individual; and 2) if the information involved is personal in nature. The information can be recorded in any form.

[9] In this matter, the mayor read aloud both letters, which named the Complainant, at the public meeting on August 21, 2021. The Village confirmed it posted the administrator's letter on its website for several days. The Complainant was identifiable through these actions.

[10] The administrator's letter contains opinions they had about the Complainant's motives, such as their "goal was to undermine everything council and office staff did", and "[their] latest barrage may have been spurred by a request for information that we denied [them]". These were opinions the administrator had about the Complainant. This qualifies as "personal information" as defined by section 23(1)(h) of LA FOIP 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:
>
> …
> (h) the views or opinions of another individual with respect to the individual;

[11] Based on the Village's submission, it appears they took their actions to demonstrate the need for the Village to have a stronger anti-harassment policy. That is, the mayor read the letters regarding the Complainant aloud, and posted the letter about the Complainant on the Village's website, to show the public why it needed a stronger anti-harassment policy. The letters contained the Complainant's personal information; as such, the Village had the Complainant's personal information in its possession or under its control. Pursuant to LA FOIP, the Village had an obligation to protect the Complainant's personal information and required authority to disclose it.

[12] In terms of a local authority's ability to disclose personal information, section 28(1) of LA FOIP outlines 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.

[13] The Village clearly did not have the Complainant's consent, and section 29 would not apply in this circumstance. From what I can tell, the Village also had no authority pursuant to

section 28(2) of LA FOIP to either read the administrator's letter at a public meeting, or to post it to the Village's website. The Village also did not state it had authority pursuant to LA FOIP to do so. As such, the Village breached the Complainant's personal information, and I, therefore, find a privacy breach occurred. The Village does not dispute this fact.

[14] I add that while section 120(1) of *The Municipalities Act* requires that council or council meetings conduct their meetings in public, section 120(2) of *The Municipalities Act* provides that meetings may be closed to the public if the matters being discussed are within the exemptions in Part III of LA FOIP. Section 120(2) of *The Municipalities Act* provides as follows:

> **120**(2) Councils and council committees may close all or part of their meetings to the public if the matter to be discussed:
>
> (a) is within one of the exemptions in Part III of *The Local Authority Freedom of Information and Protection of Privacy Act*;

[15] Part III of LA FOIP includes section 15(1)(b)(ii). Section 15(1)(b)(ii) of LA FOIP provides that a head may refuse to give access to a record that discloses agendas or the substance of deliberations of meetings where matters discussed at the meetings could be refused pursuant to Part III or Part IV of LA FOIP. Section 15(1)(b)(ii) of LA FOIP provides:

> **15**(1) A head may refuse to give access to a record that:
>
> …
> (b) discloses agendas or the substance of deliberations of meetings of a local authority if:
>
> …
> (ii) the matters discussed at the meetings are of such a nature that access to the records could be refused pursuant to this Part or Part IV.

[16] Part IV of LA FOIP includes section 28(1). Section 28(1) of LA FOIP provides that a local authority is not to disclose personal information in its possession or control without the individual's consent except if the disclosure is authorized by LA FOIP. Since Part IV of LA FOIP enables a local authority to refuse access to personal information, then council

and council committees may close all or part of its meetings to the public if the matters being discussed include personal information.

[17] In this matter, if council wanted to develop a stronger anti-harassment policy, it should have held an *in-camera* session where it could have discussed the contents of the letters regarding the Complainant. Such a meeting should have considered the principles of *need-to-know* and *data minimization* that underlie Part IV of LA FOIP. *Need-to-know* requires that a local authority only discloses on a need-to-know basis, while *data minimization* requires a local authority to disclose the lease amount of personal information necessary for the purpose. In my office's Review Report 282-2018 regarding the Rural Municipality of Parkdale No. 498, I outlined at paragraph [42] four steps rural municipalities should take to ensure it meets these principles as follows:

> …
> 1. If a R.M. council is discussing correspondence or a matter that contains sensitive personal information (such as health or financial information), the best practice is for the R.M. to provide council members with a redacted version of the personal information, or only the personal information that is necessary for the discussion. The discussion should be closed to the general public or held in camera. After coming out of the closed meeting, the R.M. should then pass a motion with basic or no personal information.
>
> 2. In meeting minutes, the R.M. should record the least amount of personal information, although best practice is to record no personal information. For example, the R.M. could in its minutes refer to "an Applicant", "a Complainant", "a Rate payer", "a Tax payer" or could use the initials of the person it is discussing.
>
> 3. If council includes personal information in its minutes, then before posting to its website, the best practice is to redact that personal information.
>
> 4. To help the public determine what personal information they provide to the R.M., the R.M. should provide notice, such as through pamphlets or information on its website, to the public about how the R.M. may include the personal information as part of public council or committee agenda meetings, or that the R.M. may publish it to its website. Such notice is in accordance with subsection 25(2) of LA FOIP, which provides:
>
> > **25**(2) A local authority that collects personal information that is required by subsection (1) to be collected directly from an individual shall, where reasonably practicable, inform the individual of the purpose for which the information is collected.

[18] Having stated this, when a privacy breach is confirmed, my office then moves on to consider how the public body addressed the breach, which is what I will now do.

[19] 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.

[20] I will now assess these four areas. I will provide any recommendations I feel are necessary to make at the conclusion of this Report.

Contained the breach as soon as possible

[21] Upon learning that a privacy breach has occurred, steps should be taken to immediately contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; and
- Correcting weaknesses in physical security.

(*Privacy Breach Guidelines*, p. 4)

[22] Effective and prompt containment may reduce the magnitude of a breach and, in some instances, the risk to individuals.

[23] As mentioned previously in this Report, the mayor read both letters regarding the Complainant aloud at a public meeting, and then had the administrator post the administrator's letter to the Village's website. Although the Village stated, "no records, per se, were involved in the breach…", there were records involved – the letters naming the Complainant. The Village even posted one of the letters on its website. Once the Village posted the administrator's letter on its website, it lost control over who could copy and further disseminate that letter during the period the letter was accessible.

[24] Further, the act of publicly disclosing personal information aloud carries many inherent risks when it comes to later containing that information. For one, it is difficult to ask people to unhear what they have already heard. Once people hear something, they can take that information and continue to disseminate it beyond the control of the local authority.

[25] People may also record public meetings, without the local authority's knowledge, which appears to have been the case in this matter. The Complainant provided my office with an audio recording of the meeting which someone else (i.e. someone not affiliated with the Village office or council) had made. Again, such a recording becomes something that can exist beyond the control of the local authority. While a local authority can ask the individual to delete the recording, it needs to be aware the individual made the recording in the first place.

[26] Regardless, in this matter, the Village stated its privacy officer discovered the privacy breach (the administrator's letter on the website) on August 24, 2021, and that it took the letter down September 7, 2021. The Village did not say why it took it so long to do so. The Village also made no public announcements about the breach and did not report the breach to my office, despite acknowledging that it was a violation of its own privacy bylaws. The Village made minimal steps at containment, and given the methods of disclosure, likely had minimal ability to contain the breach. As such, I find the Village did not take adequate steps to contain the breach.

Notified the affected individual as soon as possible

[27] It is a best practice to inform affected individuals and my office of a privacy breach. The following is a list of individual organizations that may need to be notified as soon as possible after learning of the incident:

- The organization's privacy officer
- My office
- The police, if criminal activity is suspected and
- The affected individual(s) (unless there are compelling reasons why this should not occur).

(*Privacy Breach Guidelines*, pp. 4 to 5)

[28] Providing notice 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 the affected individuals directly.

[29] In this matter, the Village stated it did not provide notice to the Complainant because the Complainant was "certainly aware". The Village added as follows:

> …
> Both staff and Council feel strongly that notifying the complainant of the breach will be seen as a "win" [by them] and will encourage [them] to continue [their] aggressive behavior.
>
> Any damage that might occur to the complainant would be damage to [their] reputation, but frankly, the damage is caused by [their] own actions. The breach only made people aware of the impact of that behavior.

[30] In correspondence dated September 7, 2021, the Complainant stated to the Village as follows:

> …
> Council's decision to hold a Public Meeting on August 21, 2021 at the Village's Fire Hall, where the Administrator's letter was read aloud wherein [their] feelings and opinions were openly discussed and wherein [their] letter openly named me as the cause of [their] distress; I strongly object to this unacceptable and offensive treatment of me by Councillor [name redacted] of the Resort Village of Kivimaa-Moonlight Bay, and I expect that Council will take appropriate actions to remedy the situation. Defamation of my character will not be tolerated.

> By holding the Public Meeting where Councillor [name redacted] participated at this meeting where I was maligned and discredited, it is unprincipled and improper. In following The Municipalities Act, Councillor [name redacted] should have declared that he will abide by the requirements and statements in the Oath of Affirmation. I am asking Council to acknowledge that the actions of Councillor [name redacted] were inappropriate. I am also asking Council to address these concerns and take the necessary steps to rectify the situation while applying The Municipalities Act, Bylaws, Procedures and any Policies of the Village, and the Local Authority Freedom of Information and Protection of Privacy Act…

[31] In response, the Village stated as follows in a letter to the Complainant dated October 18, 2021, and signed by the mayor:

> …
> Thank you for your letters dated September 7, 2021. They have bene distributed to each council member and the administrator.
>
> Council has read the letters and reviewed your requests and have decided that no further action is required.

[32] At times, local authorities face unwanted criticism they may feel borders on harassment. In some respects, local authorities need to be prepared to accept such criticism as it is part of the democratic process. If behaviours from the public go overboard, then local authorities have remedies to deal with issues that arise including implementing anti-harassment policies. If the situation warrants, local authorities can also involve law enforcement. In this matter, the Village chose to personalize the matter by willfully disclosing, without authority, the Complainant's personal information in an apparent attempt to neutralize their behaviour.

[33] Even though the Complainant was fully aware of the breach, the Village still had an obligation to address the Complainant's concerns regarding the breach. That is, the Village should have at least acknowledged to the Complainant that it did breach their privacy, and that its actions violated LA FOIP. The Village, though, appears to believe it was justified in its actions. From an accountability perspective, this is distressing. Individuals should feel confident that public bodies will take the necessary steps to meet their legislative obligations in protecting personal information, which I outlined at paragraph [17] of this

Report. At the very least, the Village could have offered an apology for its actions, and provided reassurances to the Complainant, and all its constituents, that it has more regard for peoples' personal information than it showed in this matter.

[34] I find the Village did not provide proper notice.

Investigated the breach

[35] Investigating the privacy breach to identify root causes is key to understanding what happened. It is an important step in mitigating the risk of a future breach of a similar nature from occurring. 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?

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

[36] In its submission, the Village stated there were no issues of a technical or administrative nature. The Village added as follows:

> The root cause of the breach was the intense frustration generated by the complainant's ongoing harassment and bullying of staff in [their] continual vendetta against the current Council.

[37] Again, anyone who works for, or is an official of, a local authority may at some time face public scrutiny that appears to border on harassment. The frustration it can generate is understandable. It, however, does not release a local authority of its obligation to protect personal information. The Village admits that it did not follow its own privacy bylaws and willfully breached the Complainant's personal information – this is the actual root cause of this privacy breach. It is not apparent to me that the Village understands this, or that it could have dealt with the situation differently such as through an *in-camera* session. For these reasons, I find the Village did not conduct an adequate investigation.

Taken steps to prevent future breaches

[38] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. Essentially, this is what steps can be taken to prevent a similar privacy breach from occurring. To assist, some questions trustees can ask are:

- 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*, p. 7)

[39] In terms of prevention, the Village submitted as follows:

> Both Council and employees are aware of the requirements of the Freedom of Information and Protection of Privacy Act. By instituting an Anti-Harassment Bylaw, the Village will have a legal means of stopping unacceptable actions by individuals, whether they are Council, staff or ratepayers. We have also installed a camera in the office to monitor all behavior by both ratepayers and staff – this should prevent any "he said, she said" disagreements.

[40] Contrary to what the Village states, it again seems to me that it does not fully understand its obligations to protect personal information pursuant to LA FOIP. If the Village felt it needed a stronger anti-harassment policy, then it should have contemplated how it could implement such a policy without violating the Complainant's privacy. Local authorities will always need to deal with individuals or situations they feel are problematic, but they cannot commit privacy breaches to address them. Based on the Village's actions and statement, I find it does not have an adequate plan for prevention.

[41] Further, I add that installing cameras raises additional levels of concern over privacy. By doing so, the Village now needs to be mindful of the video it captures and how it manages or retains recordings as they may also contain personal information. The Village also needs to be aware of how it uses or discloses information from recordings, and whether it makes its ratepayers aware that it is capturing that information and for what purposes. I suggest the Village refer to my office's Video Surveillance Guidelines for Public Bodies to ensure its use of a surveillance camera and its associated policies align with its obligations pursuant to LA FOIP.

[42] As the Village states it has a privacy bylaw that aligns with LA FOIP, then I recommend it review its bylaws to ensure they address its obligations regarding how to manage personal information, including when to do so *in-camera* as I outlined at paragraph [17] of this Report. I also recommend the Village provide its staff, mayor and councillors with LA FOIP training so that everyone understands their obligations pursuant to LA FOIP. My office provides many resources that support such knowledge, including:

- What Councillors Should Know about LA FOIP
- LA FOIP 101 - Webinar, The Basics for Cities, Towns and Municipalities
- Blog, Rural Municipalities – so, how should you manage personal information?

[43] Finally, I recommend the Village provide a written apology to the Complainant.

III FINDINGS

[44] I find I have jurisdiction.

[45] I find that a privacy breach occurred.

[46] I find the Village did not take adequate steps to contain the privacy breach.

[47] I find the Village did not provide adequate notification.

[48] I find the Village did not properly investigate the privacy breach.

[49] I find the Village did not take appropriate steps to prevent similar privacy breaches from occurring.

IV RECOMMENDATIONS

[50] I recommend the Village review its bylaws to ensure they address its obligations regarding how to manage personal information, including when to do so *in-camera* as I outlined at paragraph [17] of this Report. I also recommend the Village provide its staff, mayor and councillors with LA FOIP training so that everyone understands their obligations pursuant to LA FOIP.

[51] I recommend the Village provide written apology to the Complainant.

Dated at Regina, in the Province of Saskatchewan, this 6th day of September, 2022.

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