



INVESTIGATION REPORT 350-2017

Village of Hodgeville

August 16, 2018

Summary:

The Complainant submitted a breach of privacy complaint to the Village of Hodgeville (the Village) regarding the Village's practices for handling Code of Conduct complaints. The Village did not respond to the Complainant's privacy breach complaint and instead forwarded the complaint to the personal email accounts of all Village Councillors and encouraged the complaint be shared on social media. The Commissioner found that the Village did not appropriately respond to the Complainant's privacy breach complaint and that the Village did not have authority for the disclosure of the complaint. The Commissioner made a number of recommendations including having appropriate policies for the collection, use and disclosure of personal information when handling Code of Conduct complaints and implementing mandatory annual access and privacy training for all employees and Councillors. The Commissioner also recommended the Village establish a records retention schedule and implement a policy to discourage the use of personal email accounts for official business.

I BACKGROUND

- [1] On November 21, 2017, the Complainant submitted a breach of privacy complaint to the Village of Hodgeville (the Village) regarding how the Village handles Code of Conduct complaints. Rather than responding to the Complainant's privacy breach complaint, the Village forwarded the complaint to the personal email accounts of all Village councillors and encouraged the complaint be shared on social media.
- [2] In early December, the Complainant submitted a letter requesting my office investigate this complaint.

[3] On January 23, 2018, my office notified both the Village and the Complainant of my intentions to undertake an investigation. In the notification emails, my office requested the Village address why it had not responded to the Complainant and whether or not the Village believed a breach of privacy had occurred.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction to conduct an investigation?

[4] The Village is considered a local authority pursuant to subsection 2(f)(i) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). Thus, I have jurisdiction to conduct this investigation.

2. Did the Village respond appropriately to the Complainant's privacy concern?

[5] After receiving the Complainant's request, my office inquired if the Village had responded to the complaint, or if it intended to. The Village indicated that it did not believe the complaint was related to a privacy breach and did not intend to respond.

[6] Part IV of LA FOIP outlines the obligations of a local authority to protect personal information. If an individual has concerns with a public body's collection, use, disclosure or safeguarding of their personal information, the individual can request the public body address their concerns. It is best practice for the public body to respond within 30 days, addressing the individual's privacy concern and advising the individual of their right to request my office investigate the matter if they are not satisfied with the response.

[7] When a public body receives an alleged breach of privacy complaint, the first action they should take is to investigate to determine if a privacy breach has occurred. If the public body's internal investigation concludes that the alleged breach of privacy complaint is unfounded, it should provide reasons to the individual as to how it arrived at this conclusion. Reasons might include: the information does not qualify as personal information under LA FOIP; they had authority under LA FOIP; or they had consent from

the individual to disclose. If a public body finds that a breach of privacy has occurred, it should explain what happened, the findings of their investigation and outline steps taken to prevent future occurrences.

- [8] It is best practice for a public body to respond to an individual's privacy breach complaint, whether the public body is of the opinion it is valid or not. As such, the Village did not respond appropriately to the Complainant's privacy breach complaint.

3. Did a privacy breach occur?

- [9] The Complainant's request for my office to investigate their breach of privacy concern provided the following:

The Confidential Letter to Mayor [name of Mayor] and CAO [name of Chief Administrative Officer] including attachments was hand delivered... in a sealed envelope labelled Private and Confidential on November 21, 2017 at about 2:30 pm at the Village of Hodgeville office. This letter clearly tells the story of the Breach of Privacy...

At 3:10 pm that same day, Mayor [name of Mayor] sent an email out from his personal email addressed to all of Council and the Village of Hodgeville office account, accessible then by the clerk. Attached to the email was the Confidential Letter from [name of Complainant] submitted only 40 minutes earlier...

That evening at the Regular Village of Hodgeville Council Meeting, as I walked into the meeting hall at about 6:45 pm, I found many copies of my confidential letter... scatter around the hall and meeting area. The public present were reading the confidential document...

- [10] The *confidential letter* referred to by the Complainant is the breach of privacy complaint submitted to the Village. In the complaint letter submitted to the Village, the Complainant outlines concerns about how the Village handled a Code of Conduct complaint that the Complainant had submitted due to concerns with another council member. The complaint letter indicates that the Code of Conduct complaint was discussed at a public meeting, rather than *in camera*, and a delegate at the meeting was provided an opportunity to address council at the public meeting and included complaints against the Complainant.

- [11] Based on the response from the Village, a privacy breach investigation into the complaint was not conducted as the Village was of the opinion that a breach of privacy had not occurred. As noted earlier in this report, when a public body received an alleged breach of privacy complaint, the first action it should take is to undertake an investigation to determine if a privacy breach occurred. This would include determining if the information at issue qualifies as personal information, if the personal information was collected, used or disclosed, and if so, was there authority to do so.
- [12] There are two different privacy concerns being considered in this investigation. First, the Complainant has concerns about the Village's practice of discussing Code of Conduct complaints at public council meetings, rather than discussing *in camera*. Concerns of the Village's practice of handling Code of Conduct complaints is also discussed in Investigation Report 349-2017. Second, the Complainant's privacy breach complaint that was submitted to the Village was shared with others.
- [13] In order for a privacy breach to occur, the collection, use and disclosure of information must involve an identifiable individual's personal information/personal health information.
- [14] In the Village's submission, it took the position that the complaints submitted by the Complainant did not contain the Complainant's personal information as defined at subsection 23(1) of LA FOIP.
- [15] Subsections 23(1), (f), (g) and (k)(ii) of LA FOIP 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, and includes:

...

(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;

...

(k) the name of the individual where:

...

(ii) the disclosure of the name itself would reveal personal information about the individual.

[16] Subsection 23(1) of LA FOIP provides a list of examples of information that would qualify as personal information, however the list is not exhaustive. There can be other types of information that would qualify as personal information that are not listed. Part of that consideration involves assessing if the information has both of the following:

1. Is there an identifiable individual?

Identifiable individual means that it must be reasonable to expect that an individual may be identified if the information were disclosed. The information must reasonably be capable of identifying particular individuals because it either directly identifies a person or enables an accurate inference to be made to their identity when combined with other available sources of information (data linking) or due to the context of the information in the record.

2. Is the information personal in nature?

Personal in nature means that the information reveals something personal about the individual. Information that relates to an individual in a professional, official or business capacity could only qualify if the information revealed something personal about the individual for example, information that fits the definition of employment history.

[17] Individuals can submit Code of Conduct complaints regarding council members to the Village. These complaints detail actions or behavior of the council member and can result in reprimand actions against the Councillor documented in public documents. In this case, the Complainant had both a complaint against them filed by an individual and the Complainant filed a complaint against the Mayor. The Code of Conduct complaint submitted by the individual contained personal information about the Mayor, but also identified the Complainant as the individual that submitted the Complaint.

[18] The complaint against the Complainant contained the Complainant's personal information and based on discussion resulted in reprimand actions against the Complainant that were

detailed in public documents. As the Complainant was named, there is an identifiable individual. A Code of Conduct complaint was submitted to the Village regarding the Councillor's actions when responding to an inquiry about services provided by the Village. Based on the Code of Conduct Complaint and discussions in the public meeting, the Village recorded reprimand actions against the Councillor because of the complaint that was submitted. While the Complainant was acting in their role as a Councillor, how well they perform in that role and any reprimand actions taken against them based on their performance is personal in nature. As such, this information would qualify as personal information.

[19] The Complainant submitted a breach of privacy complaint to the Village regarding their practice of handling Code of Conduct complaints. It has long been the opinion of this office that the identity of an individual who has submitted an access to information request or breach of privacy complaint to a public body is considered to be personal information of that individual. As such, the identity of the Complainant as an individual that submitted a breach of privacy complaint would qualify as the individual's personal information.

[20] Next, I will consider the actions taken with the Complainant's personal information to determine if a privacy breach occurred. While there are times that a public body may have the authority to collect, use or disclose personal information, my office's resource *Privacy Breach Guidelines for Government Institutions and Local Authorities* (Privacy Breach Guidelines), discusses when these actions could result in a breach of privacy:

Collection: A privacy breach can occur if a public body asks for or collects more personal information needed for the purposes for which it is being collected...

Use: A privacy breach could occur when personal information already in the possession or control of the public body is used for reasons that are not consistent with the purpose for which they were collected...

Disclosure: A privacy breach could occur when an unauthorized disclosure of personal information transpires.

- [21] In this case, the Complaint had concerns with the use and disclosure of their personal information in the Code of Conduct complaint process and in the handling of their breach of privacy complaint.
- [22] The Village's submission provided that there was nothing in Part III of LA FOIP that exempted the Village from disclosing the complaint submitted by the Complainant.
- [23] At the time the Code of Conduct complaint was submitted, the Village's Code of Ethics Bylaw provided that "all discussions surrounding alleged and substantiated contraventions of this policy shall be conducted in an *in camera* session at a council meeting."
- [24] The Village's submission argued that it had since changed the bylaw to read that these *may* be dealt with *in camera* as it was of the opinion that neither LA FOIP nor *The Municipalities Act* provided that these matter must be dealt with *in camera*.
- [25] The Government of Saskatchewan website includes a number of resources for municipalities. One of the resources available is the *Sample Template for Council Code of Ethics Bylaw*. At Part II of the template bylaw, Contravention of the Code of Ethics, it outlines a process to address contraventions and includes a disclaimer. This Part of the sample bylaw provides:

PART II CONTRAVENTION OF THE CODE OF ETHICS

(The Act requires a process to address contraventions to the code of ethics be in place but does not prescribe a set or uniform process. Below is a potential procedure for handling allegations of contravening the code of ethics. A municipality is free to decide the process under which allegations are to be received, handled, and addressed. Work with your legal counsel to ensure your procedure addresses the specific needs and capabilities of your municipality.)

Complaint Procedure

3. As required by clause (66.1(5)(c) of The Cities Act/93.1(5)(c) of The Municipalities Act/ 107.1(5)(c) of The Northern Municipalities Act, 2010), the following section details the procedure for handling contraventions of the code of ethics.

(a) To report an alleged contravention of the code of ethics, an individual/organization/member of council may submit the form found in Schedule A, by sending the form directly to (insert applicable position for receiving the complaints – i.e. municipal administrator, city clerk), by mail, e-mail, fax or courier. The complaint will then be presented to council at the next regular meeting of council in an *in camera* session.

(b) Upon receipt of a complaint, Council shall discuss the complaint and take all necessary steps to ensure the complaint is valid.

(c) All discussions surrounding alleged and substantiated contraventions of this policy shall be conducted in an *in camera* session at a meeting of council.

...

[26] Obviously if a citizen has a concern regarding Code of Conduct contraventions and they choose to submit those concerns to the Village, the Village will be collecting the information from that individual. I see no issue with the collection of information for this purpose, however the Village has an obligation to notify citizens of how that information will be used and disclosed in order to investigate these concerns. I will further discuss providing notice to individuals later in this report.

[27] Based on the advice provided by the Ministry of Government Relations in this template, these matters should be discussed by council in an *in camera* session.

[28] Subsection 120(1) of *The Municipalities Act* provides:

120(1) Subject to subsections (2) and (3), councils and council committees are required to conduct their meetings in public.

(2) Council 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*; or

(b) concerns long-range or strategic planning.

[29] As subsection 120(2) of *The Municipalities Act* provides that council may conduct portions of a meeting that are exempt under Part III of LA FOIP *in camera*. Subsection 15(1)(b) of LA FOIP is one of the exemptions included in Part III of LA FOIP and 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:

(i) an Act authorizes holding the meetings in the absence of the public; or

(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.

[30] Subsection 15(1)(b)(ii) of LA FOIP points to Part IV of LA FOIP. This Part of the legislation deals with the protection of privacy. Taking into consideration subsection 15(1)(b)(ii) of LA FOIP along with subsection 120(2) of *The Municipalities Act*, a public meeting could be closed for the purposes of protecting personal information, as provided in Part IV of LA FOIP.

[31] Subsection 28(1) of LA FOIP is found in Part IV and provides:

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.

[32] While *The Municipalities Act* provides the head of the Village with the ability to exercise their discretion about whether or not to close a meeting, it would be best practice for the Village to discuss Code of Conduct complaints in a closed meeting. If the head deems it necessary to either discuss the matter in a public meeting or include information regarding the matter in public documents, it would be best practice for the Village to first consider if there was authority for the disclosure in LA FOIP. If there was authority for the disclosure of personal information, the Village should also consider the need-to-know and data minimization principles to ensure only the personal information required is disclosed to those with a need for the information.

[33] In Investigation Report 237-2016, my office provided the following advice regarding the discussions or personal information in a public council meeting and information recorded in minutes:

[14] The RM indicated that subsection 120(1) of *The Municipalities Act* requires council meetings to be public and that section 117 of *The Municipalities Act* requires council minutes to be public documents after adoption.

[15] Subsection 28(1) of LA FOIP provides that a local authority may disclose personal information with the consent of the individual or in accordance with section 28 of section 29 of LA FOIP. Since the Complainant in this case did not provide consent for the disclosure, I must determine if there was authority for the RM to disclose personal information pursuant to section 28 or section 29 of LA FOIP.

...

[18] Based on subsection 28(2)(r) of LA FOIP and subsection 117(1)(d) of *The Municipalities Act*, the RM has the authority to disclose the Complainant's personal information in its Council meeting minutes.

[19] I find that the RM had authority to disclose the Complainant's personal information in its Council meeting minutes.

[20] I note, though, that the purpose of LA FOIP is to ensure that local authorities operate transparency while ensuring those same local authorities protect the privacy of Saskatchewan residents. So while I support local authorities in publishing its council meeting minutes on its website, I also encourage that they implement measures to protect the privacy of Saskatchewan residents.

[21] So while I find that the RM has authority to disclose the Complainant's personal information pursuant to subsection 28(2)(r) of LA FOIP and subsection 117(1)(d) of *The Municipalities Act*, I suggest the RM de-identify or redact the personal information when publishing the meeting minutes to its website. Below are a few best practices I recommend the RM undertake.

[22] First, the RM should provide notice to the public about how personal information submitted to it could become a part of public council or committee agendas of meetings, and could also be published to the RM's website. Such a notice would be 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.

[23] The notice can appear on brochures, its website, or any other medium that contains the contact information of the RM and/or council members' contact information. This notice will help residents determine what personal information they will include in their correspondence to the RM.

[24] Second, if the correspondence contains sensitive personal information (such as health or financial information), then the RM should provide council members with a

redacted version of the information for the council meeting, such as agendas. If council members need to know the sensitive personal information in order to make a decision, then council should consider closing the council or committee meeting to the public.

[25] Third, the RM should record the least amount of personal information necessary in its council meeting minutes. For example, an RM could in its minutes refer to “an Applicant”, “a Complainant”, “a Rate payer”, “a Tax payer” or could use the initials of the person they are dealing with.

[34] The breach of privacy complaint submitted by the Complainant raised concerns about how Code of Conduct complaints were handled by the Village. An individual has a right to submit a privacy breach concern to a public body regarding any practice they undertake. The Village has a corresponding obligation to respond to the Complainant’s concerns and treat the identity of the individual as personal information. It is best practice for public bodies to consider who has a need-to-know information about the complaint in order to provide an adequate response and only use or disclose the information required to investigate the matter. Forwarding an email to all council members encouraging them to share the breach of privacy complaint and post to social media is not an appropriate disclosure of information.

[35] Based on the Village’s submission, it does not appear that any consideration for authority under LA FOIP or privacy best practices were considered before it used and disclosed the Complainant’s personal information. While there may be exceptions in LA FOIP that could provide authority for use or disclosure in this instance, the Village would have needed to make these considerations prior to taking any action with the personal information. As such, I find that multiple privacy breaches have occurred.

[36] I recommend that the Village create a policy for the processing of access to information requests and privacy breach complaints. The policy should ensure that the Village has, in each case, appropriate authority for the collection, use and disclosure of the personal information (personal information includes the individual’s identity) and has considered the need-to-know and data minimization principles.

- [37] I recommend that the Village amend its bylaw to provide that Code of Conduct complaints will be dealt with in a closed meeting.
- [38] I recommend that the Village develop and implement a policy for the collection, use and disclosure of personal information for the purposes of managing the Code of Conduct complaints. The policy should ensure that the Village has appropriate authority for the collection, use and disclosure of the personal information involved and has considered the need-to-know and data minimization principles.
- [39] I recommend that the Village include a notice on its complaint forms as to how information submitted will be used or disclosed.
- [40] I recommend that the Village implement mandatory annual access and privacy training for all Village employees and councillors
- [41] I recommend that the Village issue an apology to the Complainant for the disclosure of their privacy breach complaint.

3. Use of personal email accounts for official Village business.

- [42] When the Mayor forwarded the Complainant's privacy breach complaint to other Councillors, it appears that the Mayor used a personal email account. Further, the email accounts for the Councillors were personal/business email accounts. My office has issued a number of reports on the use of personal email accounts. Investigation Report 101-2017 is a recent report that was issued that addresses this matter and provides:

[26] Personal email accounts pose information security risks for government records. For example, records could end up stored on email servers that are outside Canada. In instances where webmail services are used, such as Gmail or Hotmail, email content is scanned and read in order to provide targeted advertising. Personal information in those records is not only stored outside Canada but is also disclosed to the webmail provider. Government institutions are required under FOIP to take reasonable security measures to protect personal information from unauthorized access, collection, use or disclosure. When government records are stored in a personal email account with data

servers located outside of Canada, the government no longer has control of how that information will be protected, disclosed, or accessed.

[27] In this case, the Minister's personal/business email account was a "sasktel.net" account. According to SaskTel's website, some SaskTel data is stored outside of Canada...

...

[33] Finally, the practice of using personal email for government-related activities threatens the proper functioning of FOIP which requires that public bodies respond to written access to information requests openly, accurately and completely. The use of personal email accounts by public servants makes this duty difficult to comply with because government may not be aware of the existence of emails on personal email accounts that are responsive to an access request.

[43] The Mayor forwarded a copy of the complaint from what appears to be a personal @sasktel.net email account to the Village's @sasktel.net email account, as well as the personal email accounts of the councillors. Three email accounts are @hotmail.com and two are @sasktel.net email accounts.

[44] When asked why the councillors use personal email accounts for village business, the Village simply replied that it has always been done this way. The Village also indicated it did not have policies regarding retention of email or use of personal email accounts.

[45] Prior to January 1, 2018, my office's position was that local authorities had an implied duty to protect personal information under LA FOIP. As of January 1, 2018, the duty has now been enshrined in statute at section 23.1 of LA FOIP. This section provides:

23.1 Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

(a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;

(b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the personal information in its possession or under its control;

(ii) loss of the personal information in its possession or under its control; or

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

[46] Allowing council members to use their personal accounts for official business does not provide the Village with the ability to appropriately safeguard personal information or properly retain official records.

[47] Further, subsection 116(1) of *The Municipalities Act* provides:

116(1) A council shall establish a records retention and disposal schedule, and all documents of the municipality shall be dealt with in accordance with that schedule.

[48] I recommend the Village establish a records retention and disposal schedule.

[49] I recommend the Village set up email accounts for the councillors to use when conducting business for the Village to ensure the security and retention of these records.

[50] I recommend the Village develop and implement a policy to discourage the use of personal email accounts for official business, to ensure information is appropriately safeguarded and records are retained within its own systems.

[51] I recommend the Village ensure all copies of the Complainant's privacy breach complaint be deleted from the personal email accounts involved.

III FINDINGS

[52] I find that the Village did not respond to the individual's privacy breach complaint and it should have.

[53] I find that portions of the information at issue qualifies as personal information of the Complainant pursuant to subsection 23(1) of LA FOIP.

[54] I find that the Village did not adhere to the practice detailed in their bylaw to discuss Code of Conduct complaints in a closed meeting

[55] I find that the Village did not have authority to disclose the Complainant's breach of privacy complaint.

IV RECOMMENDATIONS

[56] I recommend that the Village create a policy for the processing of access to information request and privacy breach complaints. The policy should ensure that the Village has, in each case, appropriate authority for the collection, use and disclosure of the personal information (personal information includes the individual's identity) and takes into consideration the need-to-know and data minimization principles.

[57] I recommend that the Village amend its bylaw to provide that Code of Conduct complaints will be dealt with in a closed meeting.

[58] I recommend that the Village develop and implement a policy for the collection, use and disclosure of personal information for the purposes of managing the Code of Conduct complaints. The policy should ensure that the Village has appropriate authority for the collection, use and disclosure of the personal information involved and takes into consideration the need-to-know and data minimization principles.

[59] I recommend that the Village implement mandatory annual access and privacy training for all Village employees and councillors.

[60] I recommend that the Village issue an apology to the Complainant for the disclosure of their privacy breach complaint.

[61] I recommend the Village establish a records retention and disposal schedule.

- [62] I recommend that the Village set up email accounts for the councillors to use when conducting business for the village to ensure the security and retention of these records.
- [63] I recommend that the Village develop and implement a policy to discourage the use of personal email accounts for official business, to ensure information is appropriately safeguarded and records are retained.
- [64] I recommend that the Village ensure all copies of the Complainant's privacy breach complaint be deleted from the personal email accounts involved.

Dated at Regina, in the Province of Saskatchewan, this 16th day of August, 2018.

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