Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 231-2024

City of Saskatoon

January 29, 2025

Summary: The City of Saskatoon (City) informed the Complainant of a breach of privacy of their personal information. The Complainant requested the A/Commissioner investigate the matter. The A/Commissioner confirmed a breach of privacy did occur and found the City acted appropriately to contain and investigate the breach as well as to prevent future similar breaches. However, the A/Commissioner also found that the City did not follow best practices when it notified the Complainant, and it did not notify his office of the breach. The A/Commissioner recommended that the City ensure, going forward, that its notifications to affected individuals includes the elements outlined in this Report. Finally, the A/Commissioner recommended that, within 30 days of issuance of this Investigation Report, the City ensure it reviews and amends its policies to include, as part of its procedure, to consider proactively notifying my office of breaches of privacy, when they occur.

I BACKGROUND

[1] In a letter dated August 20, 2024, the City notified the Complainant of a breach of privacy involving their personal information. The letter stated:

> On 07/15/2024, we discovered that there had been an over-share of your personal information by the City to the CUPE Sick Bank Committee. The information that was over-shared was the findings of a complaint under the [*Respectful and Harassment-Free Workplace* Policy].

[2] On September 24, 2024, the Complainant submitted an *Alleged Breach of Privacy Reporting Form* to my office.

[3] In an email sent October 2, 2024, my office informed the City that it had received a privacy complaint regarding this matter.

[4] As an early resolution measure, on October 11, 2024, the City emailed a redacted copy of its internal breach of privacy investigation report to my office and to the Complainant. The same day, the Complainant highlighted their concern that, in addition to the overshare of information indicated in the August 20 letter, the City's internal breach of privacy investigation report appeared to confirm the occurrence of another, related breach of privacy.

[5] On October 24, 2024, my office notified the City and the Complainant that my office would be undertaking an investigation.

[6] On November 25, 2024, the City provided my office with its completed *Breach of Privacy Investigation Questionnaire*.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[7] The City is a "local authority" pursuant to subsection 2(1)(f)(i) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). Therefore, I find I have jurisdiction to conduct this investigation.

2. Is the Complainant's personal information involved?

[8] When dealing with a complaint under PART IV of LA FOIP, it is necessary to first determine whether there is "personal information" involved.

[9] In its November 25, 2024 *Breach of Privacy Investigation Questionnaire*, the City identified that the following data elements were at issue:

> The personal information involved was the findings of an investigation into a complaint by employee [the Complainant] … Those were the only details overshared and no other personal information or investigation information was involved.
>
> [Emphasis added]

[10] Subsection 23(1) of LA FOIP defines "personal information" and based on the information at issue in this investigation, subsection 23(1)(c) of LA FOIP is relevant:

> **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:
>
> …
>
> (c) information that relates to health care that has been received by the individual or to the health history of the individual;

[11] The information shared relates to the health history of the Complainant. Therefore, I find that the Complainant's personal information is involved in this matter and, as such, the rules established in PART IV of LA FOIP apply.

3. Did a breach of the Complainant's privacy occur?

[12] From a review of the materials presented by the Complainant and the City, there appears to be three data transactions that are at issue, as follows:

1. On July 15, 2024, a City representative shared the Complainant's information in a Microsoft Teams chat with a union representative for the CUPE Sick Bank Committee.

2. On July 15, 2024, a union representative for the CUPE Sick Bank Committee shared the Complainant's information at the CUPE Sick Bank Committee meeting.

3. On July 16, 2024, a City representative from the CUPE Sick Bank Committee shared the Complainant's information with another City employee.

[13] The City has acknowledged it did not have authority to use the personal information for the above data transactions. Therefore, I will not need to address whether authority existed under LA FOIP.

[14] Therefore, I find that a breach of the Complaint's privacy occurred.

4. Did the City respond appropriately to the breach of the Complainant's privacy?

[15] When a local authority reports a breach of privacy to my office, its efforts to appropriately handle the breach of privacy must be evaluated. In order to be satisfied, my office must be confident that the local authority understood the seriousness of (and appropriately addressed) the breach of privacy. When a local authority discovers a breach of privacy has occurred, my office recommends it apply the following four best practices:

- Contain the breach (as soon as possible).
- Notify affected individuals (as soon as possible).
- Investigate the breach.
- Take steps to prevent future breaches.

(*Rules of Procedure*, updated January 7, 2025, p. 29)

[16] I will consider these four steps in the City's response to the breach of privacy.

Contain the breach (as soon as possible)

[17] Upon learning that a breach of privacy has occurred, a local authority should immediately take steps to contain the breach. Depending on the nature of the breach, this may include:

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that has been breached.
- Revoking access to personal health information.
- Correcting weaknesses in physical security.

(*Guide to LA FOIP*, Ch. 6, p. 236).

[18] I find that the City acted appropriately to contain the breach of privacy. I draw this conclusion based on the following efforts by the City:

- Within three days of the initial breach of privacy, the City initiated its own internal investigation and responded promptly on July 18, 2024.
- Without delay, following its own internal investigation, the City deleted the Microsoft Teams messages wherein the breach of privacy occurred.
- Within a week of the initial breach of privacy, the City ensured all members of the CUPE Sick Bank Committee had read and signed the relevant *Oath of Confidentiality.*

Notify affected individuals (as soon as possible)

[19] The following is a list of individuals or organizations that may need to be notified as soon as possible after learning of the incident:

- Your organization's privacy officer.
- The IPC …
- The police, if criminal activity is suspected (e.g. burglary).
- The affected individuals (unless there are compelling reasons why this should not occur).

(*Guide to LA FOIP*, Ch. 6, p. 237)

[20] Notifying an individual that their personal information was inappropriately accessed is important for several reasons. Not only do individuals have a right to know, but they also *need to know* to protect themselves from any potential harm that may result from the data transaction. Unless there is a compelling reason not to, a local authority should always notify affected individuals. An effective notification should include:

- 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 the affected individual because of the breach of privacy.
- Steps taken and planned to mitigate the harm and 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).
- Recognition of the impacts of the breach on affected individuals and an apology.
- Contact information of an individual within the 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.

(*Guide to LA FOIP*, Ch. 6, pp. 237-238)

[21] I find that the City acted appropriately to inform its privacy officer of the breach of privacy. I draw this conclusion based on the City's August 23, 2024 internal breach of privacy investigation report and November 25, 2024 *Breach of Privacy Investigation Questionnaire*, which both confirm notification of the breach was provided to the City's privacy officer within three days of the incidents.

[22] I find that the City did not act appropriately as it did not proactively notify my office of the breach of privacy. I draw this conclusion based on the fact the City did not proactively report the breach of privacy to my office. I recommend that, within 30 days of issuance of this Investigation Report, the City ensure it reviews and amends its policies to include, as part of its procedure, to consider proactively notifying my office of breaches of privacy, when they occur.

[23] Further, I find that the City did not take appropriate action in terms of providing notice to the affected individual (the Complainant) of the breach of privacy. My office's *Guide to LA FOIP*, Ch. 6, emphasizes at pages 237 and 238, what notifications to affected individuals should include and I have reproduced that list at paragraph [20] above in this Report. In my investigation, I expect to see a local authority's conscientious effort to ensure

this information is included in notifications to affected individuals. While I recognize and appreciate the City's efforts to notify the Complainant of the first data transaction that constituted a breach of privacy and to address their questions, several critical aspects of the required communication were absent. Specifically, I find that the City's notification efforts were inadequate as did not address or include:

- The third data transaction, which (in its August 23, 2024 internal breach of privacy investigation report) the City alleges occurred verbally during "a 1:1 meeting."
- a description of the possible types of harm that may come to the affected individual because of the breach of privacy and how they can mitigate harm. This best practice is outlined in my office's *Guide to LA FOIP*, Ch. 6, at page 237.

[24] Subsequently, I recommend that the City ensure, going forward, breach of privacy notifications to affected individuals include the elements detailed in my office's *Guide to LA FOIP*, Ch. 6, pages 237 and 238 and noted above at paragraph [20] of this Report.

Investigate the breach

[25] Once the breach has been contained and appropriate notification has occurred, the local authority must conduct an internal investigation. My office outlines specific questions to be considered as part of an effective investigation, which should address the incident on a systemic basis and include a root cause analysis. At the conclusion of its investigation, the local authority should have a solid grasp on what occurred which helps inform how to prevent future breaches (*Guide to LA FOIP*, Ch. 6, pp. 238-239).

[26] I find that the City took appropriate action in its investigation of this privacy breach. I draw this conclusion based on the following efforts by the City:

- The City conducted its own breach of privacy investigation and published an internal investigation report. The City's internal investigation report described: the nature of the incident, privacy obligations, number of employees affected, personal information involved, individuals interviewed, incident descriptions, extent of the breach, and recommendations.
- The City provided a detailed response to my office's *Breach of Privacy Investigation Questionnaire*. As part of its submission, the City also provided my

office a copy of the notes taken during the interviews conducted to produce its report. The City sufficiently identified causal factors and a root cause.

- The City delineated extensive recommendations (with tangible steps to facilitate implementation) to improve the overall functioning and handling of personal information within the City and the CUPE Sick Bank Committee. I will comment further on these recommendations later in this Report.

Take steps to prevent future breaches

[27] The most important part of responding to a breach of privacy is to implement measures to prevent future breaches from occurring. To do so, my office recommends that a local authority address the following questions:

- Can your organization create or make changes to policies and procedures relevant to this breach of privacy?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

(*Guide to LA FOIP*, Ch. 6, p. 243)

[28] I find that the City took appropriate action to prevent similar breaches of privacy from occurring in the future. I draw this conclusion based on the following efforts by the City, cited from its August 23, 2024 internal breach of privacy investigation report:

- The City designated extensive recommendations for the CUPE Sick Bank.
- The City issued detailed recommendations that focus on the functioning of human resources and its management of personal information. My office has confirmed with the City that the following recommendations proposed by the City have been (or are currently being) implemented:

    1. The City will only share necessary and required information with the Sick Bank Committee and ensure that any disclosure of personal information is authorized under LA FOIP.

    2. The Human Resources Division will provide administrative support to each committee for meeting minutes and other administrative functions.

3. The Human Resources Division will provide additional training to the Human Resources representative and designated alternate City employee sitting on any Sick Bank Committee regarding meeting processes, confidentiality, and breach of privacy awareness.

4. The Human Resources Division will provide training to each union representative and designated alternate City employees sitting on any Sick Bank Committee regarding meeting processes, confidentiality, and breach of privacy awareness.

5. The Human Resources Division will ensure there is a management representative (Manager or Director) on each Sick Bank Committee to ensure the committee stays within scope of guidelines. This recommendation would likely require an amendment or addition to the collective bargaining agreements.

6. All Human Resources Business Partners supporting client departments that have union members are to review any Sick Bank Committee guidelines annually.

7. The City will provide investigation training to all employees that are involved in workplace investigations.

[29] I commend the City for its emphasis, in its preventative measures, on "need-to-know" and "data minimization" principles, the neglect of which were central to the breach of privacy at issue which provide as follows:

- "Need-to-know" is the rule that personal information should only be available to those employees in an organization that have a legitimate need to know that information for the purpose of delivering their mandated services. The exercise of collecting, using, and disclosing personal information is always subject to the need-to-know principle (*Guide to LA FOIP*, Ch. 6, p. 23).

- "Data minimization" is the rule that an organization should always collect, use, and disclose the least amount of personal information necessary for the purpose. The exercise of collecting, using, and disclosing personal information is always subject to the data minimization principle (pp. 24-25).

IV FINDINGS

[30] I find that I have jurisdiction to undertake this investigation.

[31] I find that the Complainant's personal information was involved in this matter.

[32] I find that a breach of privacy occurred.

[33] I find that the City took reasonable steps to contain the breach of privacy.

[34] I find that the City did not follow best practices when it notified the Complainant of the breach of privacy and when it did not notify my office.

[35] I find that the City appropriately investigated the breach of privacy.

[36] I find that the City appropriately took steps to mitigate the breach and prevent future similar breaches of privacy from occurring.

V RECOMMENDATIONS

[37] I recommend that the City ensure, going forward, that its notifications to affected individuals include the elements outlined at paragraph [20] of this Report.

[38] I recommend that, within 30 days of issuance of this Investigation Report, the City ensure it reviews and amends its policies to include, as part of its procedure, to consider proactively notifying my office of breaches of privacy, when they occur.

Dated at Regina, in the Province of Saskatchewan, this 29th day of January, 2025.

Ronald J. Kruzeniski, KC
A/Saskatchewan Information and Privacy Commissioner