OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

November 6, 2025

Stephanie Nichols
Privacy Officer
City of Kamloops
e. snichols@kamloops.ca

Dear Stephanie Nichols:

Re: Breach Notification – Unauthorized Access/Sharing
City of Kamloops
OIPC File: [redacted]

I am the Investigator assigned to complete the monitoring of a privacy breach reported to this office by the City of Kamloops (the City) on October 14, 2025. This report is made pursuant to section 42 of the *Freedom of Information and Protection of Privacy Act* (FIPPA) and comments on the protective measures taken by the City under section 30 of FIPPA.

Incident Description

On October 9, 2025, the Mayor disclosed the personal information of a Code of Conduct complainant in an email to a City Councillor.

One individual was affected by the breach. The personal information inappropriately disclosed was their last name and prefix.

Protection of Personal Information

Public bodies in British Columbia have a statutory duty to protect the personal information in their custody or under their control. Section 30 of FIPPA sets out the legal requirement:

> *A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

The meaning of reasonable security in section 30 of FIPPA has been examined in a number of orders. For example, in paragraph 75 of Order F15-57, the Commissioner stated that "the adequacy of a public body's security arrangements is measured on an objective basis against a standard of reasonableness. This does not mean that security arrangements must be perfect, but it does signify a rigorous standard."

Response to the Privacy Breach

In order to assist public bodies in evaluating their compliance with the reasonable security standard, this office has described four key steps for managing a privacy breach. When a privacy breach occurs, public bodies must make every reasonable effort to recover the personal information, minimize the harm resulting from the breach and prevent future breaches from occurring. It is in this context that I have reviewed the actions of the City in response to this privacy breach.

1. **Breach Containment**

Containment is an important first step as it can help to mitigate the impact of the breach by limiting the further dissemination of the personal information at issue.

On October 14, 2025, the City wrote to the City Councillor to request they double-delete all copies of the email in their possession and remind them of their obligation to protect personal and confidential information. The Councillor confirmed they deleted the email message on the same date.

The City also wrote to the Mayor on October 14, 2025, to advise him that he had disclosed personal information in his control without authorization under FIPPA, which constituted a breach under section 36.3(1) of FIPPA. The City provided the Mayor with a detailed description of his obligations to protect personal information and provided a list of the numerous privacy training opportunities that were offered to him in the past. The City asked the Mayor to double-delete the email; however, as of the date of this closing letter, the Mayor had not responded to the request.

2. **Risk Evaluation**

In order to determine what additional steps may be immediately necessary, public bodies are expected to evaluate the risks associated with the breach. This includes determining whether the privacy breach could reasonably be expected to result in one or more of the significant harms listed in section 36.3(2)(a) of FIPPA.

The City evaluated the risks associated with the breach using the criteria for mandatory reporting and determined that the breach could reasonably be expected to result in humiliation and damage to reputation and relationships.

Based on the information that has been provided to me, the City's risk assessment seems reasonable as the personal information relates to a Code of Conduct complaint matter.

3. Notification

Notification of affected individuals can be an important mitigation strategy. In situations where a breach rises to the threshold of section 36.3(2) of FIPPA, notification is compulsory.

I have reviewed an anonymized copy of the notification letter. I can confirm that the notification contained the information and was delivered in the manner as required by section 11.1 of the *Freedom of Information and Protection of Privacy Act Regulation* (FIPPA Regulation) on October 14, 2025.

4. Prevention Strategies

Consideration of strategies to prevent a similar breach from occurring in the future is in the interest of the public body and those whose personal information is in their custody or under their control. These strategies may be necessary to meet the requirement of implementing reasonable security measures under section 30.

With respect to prevention measures, the City will continue privacy awareness training and communication for all City representatives to ensure privacy protection obligations are well understood. Elected officials have received numerous training sessions regarding their statutory obligations to protect confidential and personal information as addressed in the Community Charter and the Council Code of Conduct Bylaw.

Following a privacy breach, a public body's prevention measures are typically associated with the vulnerability that caused the breach. There are no additional physical or technological safeguards that could have prevented this breach, as the City had corporate policies, Code of Conduct bylaws and training in place to educate City staff of their confidentiality obligations. The City has provided, or offered, FIPPA and privacy training to the Mayor, as recently as October 8, 2025; therefore, the recent breach is not the result of a lack of knowledge or education made available or provided by the City.

Furthermore, section 36.2 of FIPPA requires a public body to develop a privacy management program (PMP), which includes a documented process for responding to privacy complaints and privacy breaches. The City confirmed that they have a PMP which was in place at the time of the privacy breach. In addition, the City has a separate Privacy Breach Corporate Policy that outlines the reporting requirements and processes for breaches such as this.

Conclusion

I find that the City's response to the breach was compliant with section 30 of FIPPA. I am satisfied that every reasonable effort has been made to mitigate any potential harm to the affected individual that may result from the breach and that appropriate steps have been taken to prevent future breaches of this type.

This concludes the monitoring of this privacy breach, and the above referenced file has been closed.

Sincerely,

Lisa Fleischauer
Investigator