OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

October 21, 2026

City of Kamloops
E snichols@kamloops.ca

Dear Stephanie Nichols:

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

I am the Investigator assigned to monitor the response by the City of Kamloops (the public body) to a privacy breach reported to this office on September 15, 2026.

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 public body under sections 30 and 36.3 of FIPPA.

Background

On September 13, 2026, the Mayor of Kamloops sent an email with the subject line "O'Reilly NL radio" and two attached images. The Mayor sent this email to thirteen individuals, including members of the public and the media.

According to the City, the images attached to the Mayor's email were screenshots of an email from the Chief Administrative Officer to City Council and the Human Resources Director regarding a WorkSafeBC matter, including the name of the impacted employee.

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 arrangements 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

PO Box 9038, Stn. Prov. Govt.
Victoria, BC V8W 9A4
TEL 250.387.5629
FAX 250.387.1696
info@oipc.bc.ca
oipc.bc.ca

against a standard of reasonableness. This does not mean that security arrangements must be perfect but it does signify a rigorous standard."

In this matter, there is no indication that the public body had insufficient security arrangements. Furthermore, the Mayor has previously been advised that the details of employment and WorkSafeBC matters are confidential.

Response to the 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.

The public body discovered the breach on September 15, 2026. The public body tried to contain the breach by contacting the recipients of the breach and directing them to double-delete information that was disclosed inappropriately. Of the thirteen recipients, eight responded and complied. For the remaining five recipients, the City sent a Demand Notice under section 73.1 of FIPPA. At the time of writing, the City has not received compliance from these recipients.

The City can ask the Attorney General to enforce its section 73.1 demands and this is the primary mechanism in FIPPA for public bodies to seek the return or destruction of records from individuals who do not cooperate with a public body's containment efforts.

One of the recipients of the breached personal information, [redacted], published an online article questioning the City's containment attempts.[1] In addition, [redacted] published an article about the specific employee whose personal information was disclosed.[2] [redacted][3] The City views [redacted] conduct as undermining their containment efforts and exacerbating the harm caused by the breach. I agree with that assessment.

The City identified humiliation, damage to reputation and breach of contractual obligations as harms that could result from this breach. The City sent notice to the impacted individual on September 16, 2026. I have reviewed an anonymized copy of the notice and find that it includes the relevant and appropriate information.

On September 15, 2026, the public body emailed a separate letter to the Mayor. The public body wrote that the Mayor disclosed personal and sensitive information about a City employee

[1] [redacted]

[2] [redacted]

[3] The City has provided the OIPC's contact details to this individual should they wish to file their own privacy complaint under section 42(2)(e)(i) of FIPPA.

and wrote that this was a "privacy breach as defined in Section 36.3(1) of the *Freedom of Information and Protection of Privacy Act (*FIPPA)."

The public body provided the Mayor with a description of his obligations to protect personal information and provided a list of the numerous privacy training opportunities offered to him in the past.

The public body has shared that the Mayor challenged the Privacy Officer's authority to contain the breach and included members of local media in his communications questioning that authority.

To be clear, as the delegated head of the public body for privacy matters, the Privacy Officer is responsible for ensuring the public body's compliance with FIPPA, which includes its statutory obligation to protect personal information.[4] Furthermore, if they have reasonable grounds to believe that this personal information is in the possession of a person or an entity not authorized by law to possess it, section 73.1 of FIPPA authorizes them to issue a written notice demanding the return and/or deletion of that personal information. Based on the information before me, the Privacy Officer is operating within their authority and taking reasonable steps to contain the privacy breach and protect both the City and its staff.

A public body's prevention measures following a breach are typically tied with the vulnerability that caused the breach in the first place. There are no reasonable physical or technological safeguards that could have prevented this breach. The public body already had extensive policies in training in place to educate elected officials on their confidentiality obligations. This breach does not stem from a lack of privacy protections; rather, it is the direct result of the Mayor's actions.

Conclusion

I find that the public body has taken reasonable steps to mitigate potential harm to the affected individual and engaged the means available to them to attempt to prevent future breaches.

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

Sincerely,



Ryan Graves

[4] See section 30 of FIPPA.

Investigator