OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

September 1, 2026

City of Kamloops
E ngarbay@kamloops.ca

Dear Natalie Garbay:

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 by the City of Kamloops (the public body) on August 14, 2026.

On August 13, 2026, an article was published online.[1] In this article, the Mayor of Kamloops shared with the journalist a cease-and-desist letter (the Letter). The Letter instructed the Mayor to stop making "serious, unfounded" claims about staff in the City's [redacted] department. In the interview with the journalist, the Mayor claims the Letter is related to a [redacted].[2] Furthermore, the Mayor accused staff of [redacted]

While the media article does not explicitly name the staff member, [redacted] The Mayor's discussions with the journalist thus created a [redacted]. Consequently, the City is concerned that the public could [redacted], which is a confidential employment matter.[3]

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.

Protection of Personal Information

[1] [redacted]
[2] This dispute related to the Mayor's r[redacted] containing personal information.
[3] A version of the workplace investigator's code of conduct report has been published online. However, personal identifiers of employees and witnesses were redacted in that report.

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

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

There is no indication that the public body had insufficient security arrangement and the Mayor has previously been advised that the details of the code of conduct investigation were confidential and should not be discussed publicly.

I accept that the Mayor's decision to disclose the Letter to the media, along with his comments to the media in the related interview, could indirectly disclose the personal information of the employee [redacted]. The City submits, and I agree, that the disclosure of this personal information could result in privacy related harms.

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 August 14, 2026. Typically, a public body's first step is to remove that information from the public sphere as quickly as possible. In this case, the public body concluded that contacting the journalist could draw more attention to the subject and potentially amplify the risks associated with the breach. I concur with that assessment, and I understand that the individual impacted by the breach feels the same.

Notification of affected individuals can be an important mitigation strategy. When a breach rises to the threshold of section 36.3(2) of FIPPA, notification is compulsory. The public body sent notification on August 14, 2026. I have reviewed an anonymized copy of this notification and I find that it includes the relevant and appropriate information.

On August 14, 2026, the public body emailed a separate letter to the Mayor. The public body wrote that the Mayor had "provided [redacted] with information relating to personal information of a City of Kamloops staff member, as well as sensitive employment matters". In

addition, the public body noted that the Mayor had "directly shared a City record with [redacted]… in relation to employment matters."

The public body advised the Mayor that "this situation is 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.

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, based on the information provided by the City, it appears to be the direct result of the actions of the Mayor.

Conclusion

I find that the public body has taken all reasonable steps to mitigate potential harm to the affected individual and taken all reasonable and available prevention steps. This concludes the monitoring of this privacy breach and the above referenced file has been closed.

Sincerely,



Ryan Graves
Investigator