OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

October 23, 2026

City of Kamloops
E snichols@kamloops.ca

Dear Stephanie Nichols:

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

I am the Investigator assigned to monitor the response by the City of Kamloops (the public body) to privacy breaches reported to this office on October 5 and 6, 2026. Due to the similarities between them , I will address both breaches in a single report.

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

Breach [redacted]

On October 2, 2026, an article was posted to the [redacted].[1]

The City reports that the article revealed that the Mayor had provided the author of the article, [redacted], with personal information about a former employee of the City. In [redacted] article, there is a screenshot of a text message between Councillor Mike O'Reilly and the Mayor, which includes a photograph of a printed copy of a text message between the Mayor and a former employee (Person A). The City advises that Councillor O'Reilly maintains he did not share these text messages with [redacted]. The City determined that the Mayor disclosed these messages to [redacted], who in turn published personal information about a former City employee.

In addition, the City expressed concern that the article contains other potential breaches relating to staff who were involved in the Mayor's workplace and Code of Conduct

[1] [redacted]

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

investigations. However, the City acknowledges that the above information would only constitute a breach if the information derived from the Mayor or another City source.

Based on the information before me, I cannot conclude that the inclusion of other personal information of staff members in the article is the result of information being given to [redacted] without authorization rather than [redacted] working out that information [redacted] on the basis of public information and/or other privacy breaches.

Breach [redacted]

On October 3, 2026, the same website posted an article titled [redacted]"[2] which included the following passage:

> *According to the Mayor's account, he apologized to staff in a nearby area for Sarai's behaviour. He has said that [Person B] was in the lunchroom at the time and overheard Sarai yelling. Later that day, according to the Mayor's recollection, [Person B] moved to another location within the City.*

The City reports that the above information reveals the personal information of Person B and [redacted]. The OIPC opened [redacted] to address this reported breach.

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

In these matters, there is no indication that the public body had insufficient security arrangements. The City reports that the Mayor has previously been advised that he is not authorized to disclose personal information about City staff.

Response to the Privacy Breach

[2] [redacted]

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 City submits that contacting [redacted]. I agree with the City's position, particularly given what the City has shared about [redacted] unwillingness to co-operate with City and return or destroy the personal information [redacted] received in other privacy breaches.[3]

For Person A, the City identified humiliation and damage to reputation as harms that could result from the breach. For Person B, the City identified humiliation, damage to reputation and breach of contractual obligations as harms that could result from the breach.

The City sent notice to Person A on October 5, 2026 and to Person B on October 6, 2026. I have reviewed an anonymized copy of the notice and find that it includes the relevant and appropriate information.

On October 5 and October 6, 2026, the City emailed letters to the Mayor in which it advised the Mayor that his disclosure of information and/or documents to [redacted] constituted "a privacy breach as defined in Section 36.3(1) of the *Freedom of Information and Protection of Privacy Act (*FIPPA)."

The City 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, it is the direct result of the Mayor's actions.

Conclusion

I find that the public body took reasonable steps to mitigate potential harm to Person A and Person B, and engaged the means available to them to attempt to prevent future breaches.

This concludes the monitoring of these privacy breaches and the above referenced files have been closed.

[3] I understand from the City that the individuals impacted by the breaches feel the same.

Sincerely,



Ryan Graves
Investigator