

July 30, 2026

City of Kamloops
E foi@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 by the City of Kamloops (the public body) on July 22, 2026.

On July 16, 2026, an article was published online.¹ In this article, the Mayor of Kamloops spoke with the author about a recent council meeting. According to the author of this article, the Mayor said “he is prohibited from communicating directly with [REDACTED] outside council meetings” and “reiterated that [the Mayor] is not permitted to communicate directly with [REDACTED] outside council meetings except through the Deputy Mayor.”

In addition, the article states that the Mayor told the author that “he received an email directly from [REDACTED] and asked Deputy Mayor Dale Bass to have future communications routed through her instead”.

The public body determined that these comments reflect a breach of [REDACTED] personal information on the part of the Mayor. 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

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.

¹ [REDACTED]

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 arrangements. Indeed, the public body has provided extensive training on FIPPA and confidentiality to the Mayor in the past.

The public body confirmed to me that the Mayor’s comments in the online article [REDACTED]
[REDACTED]
[REDACTED] The public body explained that [REDACTED]
[REDACTED]
[REDACTED].

A plausible argument could be made that the existence of [REDACTED]
[REDACTED]
[REDACTED].

Nevertheless, I acknowledge that members of the public who learn of [REDACTED]
[REDACTED]
[REDACTED] Consequently, I accept that any disclosure regarding [REDACTED]
[REDACTED] Thus, for the purposes of this file I will treat the Mayor’s comments as a breach of [REDACTED] personal information.²

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 July 20, 2026. Generally, when breaches occur it is critical that a public body take steps to remove that information from the public sphere as quickly as possible. In this case, the public body assessed that contacting the author [REDACTED] could draw more attention to the subject and potentially cause more harm to the individual. I agree with that assessment, and I understand that the individual impacted by the breach is in agreement.

² Even if disclosure of information did not constitute a breach of personal information under FIPPA, disclosure of such information could still be a violation of the public body’s own bylaws/rules, section 117(1) of the *Community Charter*, etc.

Notification of affected individuals can be an important mitigation strategy. Indeed, in situations where a breach rises to the threshold of section 36.3(2) of FIPPA, notification is compulsory. The public body sent notification via email on July 22, 2026. I have reviewed an anonymized copy of this notification and I find that it includes the relevant and appropriate information.

On July 22, 2026, the public body emailed a separate letter to the Mayor. The public body wrote that the Mayor had inappropriately shared “personal information pertaining to a City staff member and a sensitive employment matter”. The public body also suggested that the Mayor “may have shared or granted access to a City record, being an email you received from a City staff member”.³ The public body wrote 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 many 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. As previously mentioned, the public body already had extensive policies in training in place to educate elected officials on their confidentiality obligations. Any breach here does not stem from a lack of knowledge or education from the public body.

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

³ The public body has not taken any action to recover the record(s) from the author of the online article. Given the limited evidence that the records were shared, and the public body’s prediction that contacting the author could exacerbate any breach, this decision seems reasonable.