



ORDER F26-87

CITY OF KAMLOOPS & MAYOR REID HAMER-JACKSON

Ryan Graves
Investigator

October 9, 2026

CanLII Cite.: 2026 BCIPC 111

Quicklaw Cite: [2026] B.C.I.P.C.D. No. 111

Summary: The City of Kamloops reported that Mayor Reid Hamer-Jackson had disclosed personal information without authorization under FIPPA. The Commissioner opened an investigation of the Mayor's disclosure and the City's response to the alleged privacy breach. The Investigator determined that the Mayor disclosed the personal information of four individuals in contravention of section 25.1 of FIPPA. The Investigator also determined that the City's response to the breach complied with sections 30 and 36.3 of FIPPA. The Investigator ordered the Mayor to comply with the City's directions regarding containment of the breach and ordered the Mayor to comply with his duty not to disclose personal information obtained in the course of his duties except as authorized by FIPPA. As a condition of this order, the Investigator required the Mayor to receive written permission from the head of the public body, or their delegate, before disclosing any personal information of current or former staff.

Statue and sections considered in this order: *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, ss. 25.1, 30, 36.3(2), 36.3(5), 33(2)(a), 33(2)(c), 33(2)(d), Schedule 1 (definition of "personal information"), and *Freedom of Information and Protection of Privacy Act Regulation*, BC Reg 155/2012, s. 11.1(1)(b).

INTRODUCTION

- [1] On August 27, 2026, Mayor Reid Hamer-Jackson (the Mayor) sent an email to three members of the public and the City's legal counsel. The email included a 66-page attachment of text messages exchanged between the Mayor and a former City employee. The text messages include the personal information of that former employee and three other individuals.
- [2] On September 3, 2026, the City of Kamloops (the City) reported the above matter as a privacy breach to the Office of the Information and Privacy Commissioner (OIPC).

- [3] In the initial assessment of the breach reported to the OIPC on September 3, 2026, it became apparent to the OIPC that some of the personal information at issue was part of an earlier breach reported to the OIPC on March 25, 2026, involving similar circumstances. In response to that breach, the City sent a letter to the Mayor on March 31, 2026, advising him of the breach and his responsibilities regarding personal information. The OIPC monitored the City's breach response for compliance with the *Freedom of Information and Protection of Privacy Act* (FIPPA), and the Commissioner wrote to the Mayor and the Corporate Officer on April 10, 2026 about the need to protect personal information and to comply with FIPPA. In addition, the Mayor and the OIPC Director of Investigations had a phone call on April 13, 2026, in which the Director of Investigations clarified that personal information in the City's custody or control could only be released in accordance with FIPPA.
- [4] Given that these remedial efforts appear not to have been successful, it was determined that additional enforcement measures were needed to assess and achieve compliance.
- [5] On September 15, 2026, the Commissioner informed the Mayor and the City that the OIPC was formally investigating the breach reported to the OIPC on September 3, 2026.

METHODOLOGY

- [6] This investigation was conducted under s. 42(a) of FIPPA.
- [7] The information assessed includes both the information provided through the City's September 3, 2026 breach report and subsequent evidence gathered through emails and phone calls with the parties. Both the Mayor and the City were given opportunities to provide information and answer the OIPC's questions.¹ A copy of this report was provided to the Mayor and the City on October 5, 2026 and both parties were given until October 7, 2026, at 10 AM to provide final comment.²

ISSUES

- [8] As per the Notice of Investigation Commissioner Harvey sent to both parties on September 15, 2026, the issues are as follows:
1. Did the Mayor, as an officer of the public body, disclose personal information in contravention of s. 25.1 of FIPPA;

¹ For the Mayor, this includes at least 18 emails to me as the delegated OIPC Investigator and a phone conversation.

² All comments provided by the parties were considered and, where relevant, cited in this report.

2. Did the City's response to the alleged breach meet its legal obligations under ss. 30 and 36.3 of FIPPA.

ANALYSIS OF ISSUE 1

Did the Mayor disclose personal information?

- [9] The Mayor confirmed that on August 27, 2026 he sent an email with an attached PDF of text messages he had exchanged with a former employee of the City between October 13, 2022 and August 19, 2023.³
- [10] This email was sent to the City's external legal counsel and three private citizens. The Mayor has explained to me that these three individuals run local Facebook groups in the community.⁴
- [11] Both the Mayor and the City provided me with a copy of the August 27 email and attachment. I reviewed the text messages and confirmed that they contain personal information.⁵
- [12] I consider some of the personal information contained in these texts to be less sensitive. For instance, some are references to scheduling personal matters. However, other texts contain personal information I consider to be highly sensitive. For instance:
- a. On January 23, 2023, the texts discuss a potential code of conduct investigation involving a confrontation between a City councillor and a City staffer. Both the councillor and the staffer are named in the texts.
 - b. On June 6-7, 2023, the former City employee shares a serious health diagnosis and their recent symptoms.
 - c. On August 15, 2023, the former City employee shares details of their medical symptoms and their health treatment plans.⁶
- [13] Section 25.1 of FIPPA stipulates that an employee, officer or director of a public body or an employee or associate of a service provider must not collect, use or disclose personal information except as authorized by FIPPA.

³ As per a phone call and email conversation with the Mayor on September 23, 2026.

⁴ As per a phone call and email conversation with the Mayor on September 23, 2026.

⁵ Schedule 1 of FIPPA defines "personal information" as "recorded information about an identifiable individual other than contact information." Contact information is defined as "information that enables an individual at a place of business to be contacted."

⁶ The text messages sent to the Mayor on August 15, 2023, are the same texts that the Mayor shared with several local media outlets in March 2026.

[14] The term “officer” is not defined in Schedule 1 of FIPPA. Nevertheless, the Court of Appeal in *R v Skakun*⁷ determined that elected officials of a municipality are officers for the purposes of their individual obligations under FIPPA. The central issue in that case was whether a municipal councillor was an “officer” for the purposes of s. 30.4, which at the time stated:

An employee, officer or director of a public body or an employee or associate of a service provider who has access, whether authorized or unauthorized, to personal information in the custody or control of a public body, must not disclose that information except as authorized under this act.

[15] Section 30.4 has since been repealed and replaced with s. 25.1, but uses the same language of “employee, officer or director” to describe who is restricted from collection, use, or disclosure of personal information, except as authorized under FIPPA. Like the councillor in *Skakun*, the Mayor is an elected official of a public body and therefore an officer of the public body for the purposes of s. 25.1.

[16] Under FIPPA, personal information in the public body’s custody or control may only be disclosed pursuant to s. 33 of FIPPA. Any disclosure of personal information outside of the authorizations listed in s. 33 is a violation of s. 25.1.

[17] In my letter to the Mayor dated September 16, 2026, I asked the Mayor which provision in s. 33 of FIPPA authorized the disclosure of that personal information. The Mayor did not point to any provision in FIPPA that he believes authorized the disclosure but did explain that the purpose for which he sent the email on August 27, 2026 was to contradict a public narrative about his relationship with the former City employee. Specifically, the Mayor said he disclosed these text messages because he believes they support his stance that:

- a. he did not threaten to fire the employee, and
- b. the employee had medical issues that prevented them from continuing in their position.

[18] Based on the above motivations, it is clear that the Mayor reviewed the text messages and was aware of their contents.

[19] Though the Mayor did not point to a provision in FIPPA that authorized his disclosure, I nevertheless considered whether any provisions reflect his stated purpose for the disclosure.

⁷ 2014 BCCA 223 at para. 32 [*“Skakun”*].

Section 33(2)(a)

- [20] The Mayor has implied that there is no issue in him disclosing the text messages since his records can be requested through an access to information (Freedom of Information) request.
- [21] Section 33(2)(a) permits a public body to disclose information in accordance with Part 2 of FIPPA. Part 2 of FIPPA governs the release of information through an access request as well as what information the law requires to be withheld, which limits what can be released. The authority to determine what information can be released in response to an access request rests exclusively with the head of the public body or their delegate. The City's Corporate Officer is the head under the City's bylaws but they delegated their FIPPA authority to the City's Privacy Officer and Enterprise Risk Manager.⁸
- [22] In a letter to the Mayor dated March 31, 2026, the City told the Mayor:
- For clarity, the expression "FOI-able" does not mean records are releasable, it means they can be requested, and there is a legislated FOI process to be followed.*
- [23] When the Commissioner sent a letter to the Mayor and the City on April 10, 2026, the Commissioner made a similar point, stating that the Corporate Officer or their delegate, not the Mayor, has the legal authority to make decisions about releasing records in response to an access to information requests.
- [24] The Mayor is not the City's delegated decision maker for the purposes of responding to access requests, nor was he responding to an access request when he disclosed information on August 27, 2026. Even if the Mayor had been responding to an access request, that would not mean that the privacy protections in Part 2 of FIPPA no longer apply such that the Mayor could disclose personal information in the custody or control of the City according to his personal preferences. Part 2 of FIPPA has explicit rules limiting the release of personal information through access requests.
- [25] For the above reasons, I am of the view that s. 33(2)(a) did not authorize the Mayor to disclose this personal information.

Was disclosure authorized by s. 33(2)(c)?

- [26] I also considered the relevance of s. 33(2)(c) to the Mayor's disclosure. Section 33(2)(c) states that disclosure is authorized if the individual the information is about has identified the information and has consented in the prescribed manner to the disclosure.⁹

⁸ As per the City's explanation to me on October 6, 2026.

⁹ "Prescribed manner" refers to the rules outlined in [section 11](#) of the FIPPA Regulation.

[27] There is no evidence, and the Mayor has not argued, that any of the individuals whose personal information was involved in the disclosure identified the information or consented to it being disclosed to members of the public. For this reason, I am of the view that s. 33(2)(c) did not authorize the Mayor to disclose this personal information.

Was disclosure authorized by s. 33(2)(d)?

[28] Section 33(2)(d) of FIPPA states that a public body may disclose personal information for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose within the meaning of s. 34.

[29] It is plain and obvious that the Mayor's disclosure to local commentators for the purpose of furthering his argument in the public sphere was not the original purpose for which the personal information was provided to the Mayor.

[30] I also considered whether the Mayor's purpose for disclosure was for a consistent purpose. As outlined in s. 34, a consistent purpose is one which has a reasonable and direct connection to the original purpose and is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.

[31] A reasonable and direct connection under s. 34 must have a logical and plausible link to the original purpose and must flow or be derived directly from the original use or be a logical outgrowth of the original use.¹⁰ Additionally, former Commissioner Loukidelis accepted that an analysis can consider "whether the person concerned would expect his or her personal information to be used in the proposed way, even if that use has not been spelled out."¹¹

[32] There is no logical and plausible link between the purpose for which the personal information was provided and the Mayor's stated purpose for disclosing it, nor was one provided to me. Furthermore, the individuals whose personal information was implicated in this disclosure would not have expected their personal information to be disclosed in this way or for this purpose. For these reasons, I am of the view that s. 33(2)(d) did not authorize the Mayor to disclose this personal information.

¹⁰ [Investigation Report 00-01: Investigation into Use of Alumni Personal Information by Universities](#) dated October 25, 2000, at p. 12 of the PDF.

¹¹ [Investigation Report 00-01: Investigation into Use of Alumni Personal Information by Universities](#) dated October 25, 2000, at p. 12 of the PDF.

- [33] I have considered all other provisions listed in s. 33 of FIPPA. In my view, no other provisions are relevant. I find that the Mayor disclosed personal information in contravention of s. 25.1 of FIPPA.

ANALYSIS OF ISSUE 2

Did the City's response to the alleged breach meet their legal obligations under ss. 30 and 36.3 of FIPPA?

- [34] Public bodies in British Columbia have a statutory duty to protect 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.

- [35] Under s. 30 of FIPPA, public bodies are required to protect personal information in their custody or control by making reasonable security arrangements, which includes taking appropriate and necessary measures to respond to privacy breaches. These measures include four common steps, each of which is assessed below in relation to the City's efforts.

Containment

- [36] When a privacy breach occurs, public bodies must make every reasonable effort to contain the breach and prevent further distribution of the breached personal information. Approximately five hours after the Mayor sent his email with the attached text messages, the City sent its own email to two of the email recipients.¹² In this email, the City advised recipients that the Mayor had "disclosed sensitive personal information that he was not authorized to share" and directed recipients to "double-delete all copies of the August 27th email from [their] email inbox, sent items, deleted items, anywhere else [they] may have filed or saved the correspondence, as well as any hardcopies". The City asked recipients to confirm the above steps were completed and advised them that it "may take legal action to recover personal information".
- [37] The City also sent an email with similar instructions to the Mayor's spouse on September 2, 2026. The City sent this email because the properties of the PDF document the Mayor attached to his email listed his spouse as the "author" of that document. The Mayor has

¹² The third recipient of the Mayor's email was the City's external legal counsel, who notified the City's privacy department of the incident. An email to the fourth recipient resulted in an automated "unable to deliver" message. Through a separate process, the City later confirmed with this individual that they never received the Mayor's August 27, 2026 email.

since confirmed to me that he used his spouse's computer to create the PDF document and she was not involved in its preparation.¹³

[38] After receiving the City's emails, one recipient confirmed compliance with the City's directions on September 1, 2026. Another recipient acknowledged receipt but did not confirm compliance with the City's directions. On September 3, 2026, the City sent a Demand Notice to this recipient pursuant to s. 73.1 of FIPPA with a deadline of September 23, 2026. The recipient did not respond to this Demand Notice.

[39] The City also tried to have the Mayor contain the breach by sending him a letter dated August 27, 2026. In this letter the City wrote:

You are hereby directed to cease immediately, and not to repeat, any unauthorized disclosure, distribution, copying, forwarding, publication, display, or other release of personal information, confidential information, employment-related information, or City records. You must not disclose or make available any such information or records to any person unless the specific disclosure has been expressly authorized in advance by law or by the City. Any further unauthorized disclosure will be treated as a knowing and deliberate breach of your legal obligations, and the City will pursue all rights and remedies available to it without further notice to you.

You are further directed to immediately take all reasonable steps to recall, retrieve, delete, or secure every copy of the Attachment, and any copy of the information contained in it, that is in your possession or control or that you have caused or permitted to be disclosed to any other person. You must confirm in writing, by no later than noon tomorrow, August 28, 2026 the steps you have taken to do so and identify every person to whom you disclosed, forwarded, copied, or otherwise made available the Attachment or any information contained in it.

[40] The Mayor has confirmed to me that he did not respond to this letter.

[41] Based on the above, it is evident that the City took reasonable steps to contain the breach, albeit with mixed success due to non-cooperation from the Mayor and one of the recipients of his email.

Risk Assessment

[42] The City reviewed all text messages attached to the Mayor's August 27, 2026, email and assessed that the texts contained the personal information of four individuals. The City deemed the texts that referenced employment matters and/or medical information to be particularly sensitive. The City assessed the following types of risks:

¹³ As per a phone call and email conversation with the Mayor on September 23, 2026.

- a) Breach of contractual obligations
- b) Damage to reputation and relationships
- c) Humiliation
- d) Loss of employment, business or professional opportunities

[43] Having reviewed the information myself, I concur with the City's risk assessment. Further, the fact that the Mayor sent this information to individuals he views as public commentators on local affairs magnifies the foreseeable harm from the breach; wider dissemination and republication of the text messages was not only a possible byproduct of the disclosure but was inherent in the Mayor's stated intention for sending the email. This risk assessment informed the City's decision-making regarding notification and s. 36.3(2) of FIPPA.

Notification

[44] Notification to affected individuals is often a key tool for mitigating the harm from a privacy breach. Section 36.3(2) of FIPPA says that a public body must notify, without unreasonable delay, the affected individuals and the OIPC if the privacy breach could reasonably be expected to result in significant harm to the individual. Section 36.3(5) of FIPPA states that notification must be made in the prescribed manner.¹⁴

[45] The City has advised me that it viewed the August 27, 2026, breach as meeting the criteria of s. 36.3(2). Consequently, on September 3, 2026, the City sent notification to three individuals impacted by the breach: two current City employees and the former employee whose text messages with the Mayor were the subject of this breach. The City identified a fourth individual whose personal information was impacted but did not send notification because the City could not find reliable contact information for this member of the public.¹⁵

[46] The City's notification to the OIPC and the impacted individuals was delivered the day after the City's deadline for email recipients to respond to their containment efforts, and seven days after the breach was discovered. In my view, this is not an unreasonable delay. After all, impacted individuals may appreciate knowing whether the recipients of their personal information had deleted or destroyed that information, and the City could not share this detail until the recipients had been given a reasonable amount of time to confirm their compliance with the directions the City gave to them on August 27, 2026.

[47] I reviewed an anonymized copy of the three notification letters sent by the City. I compared the details in these letters to the requirements of s. 11.1(1) of the FIPPA

¹⁴ "Prescribed manner" refers to the rules outlined in [section 11.1](#) of the FIPPA Regulation.

¹⁵ I am satisfied that the City expended reasonable efforts to obtain contact information for this person.

Regulation and found that the letters mostly comply with these requirements. The City's notification includes the name of the public body, a detailed description of the breach and the personal information involved, confirmation that the Commissioner has been notified, contact information for the City's Privacy Officer, and a description of steps that the City has taken to reduce the risk of harm.

[48] However, I note that the City's letters did not specify the date on which the privacy breach came to the attention of the public body, as required by s. 11.1(1)(b)(ii) of the FIPPA Regulation. Given that the breach was discovered the same day it occurred, this deficiency is not particularly damaging to the City's efforts to mitigate harm through notification. Nevertheless, to fully comply with s. 36.3(5) of FIPPA, the City sent a follow up to the three affected individuals on October 1, 2026, and clarified the date the City discovered the breach.

[49] I also note that the City's notification letter did not provide the affected individuals with a description of steps, if any, that they could take to reduce the risk of harm that could result from the privacy breach. I think the City's choice to omit this from the letter is appropriate and permitted under s. 11.1(1)(b)(vii) of the FIPPA Regulation as it is not clear what possible steps the City could recommend in this circumstance.

Prevention

[50] The final step public bodies should take after responding to a privacy breach is implementing safeguards to prevent further breaches. A public body's prevention measures following a breach typically address the vulnerability that caused the breach in the first place. For instance, if records containing personal information are taken from a cabinet, a common-sense prevention measure would be to store the documents in a locked cabinet and locked room going forward.

[51] In this case, I see no reasonable physical or technological safeguards that could have prevented the breach. The City has not suggested that the Mayor inappropriately accessed or retained this information on his phone, only that he disclosed it inappropriately.

[52] In some cases, an employee or officer's disclosure of personal information in their custody suggests a lack of training or knowledge on their part, which can be remedied with specific privacy education and training. However, all evidence before me suggests that this was not the case for the Mayor.

[53] According to the City, the Mayor was provided with information on numerous occasions about the privacy duties imposed on him under FIPPA, including:

- **November 2022:** the City's legal counsel provided information on FIPPA and confidentiality to members of council.
- **February 2023:** the City's Privacy Officer emailed officials to outline their statutory duties under FIPPA.
- **May 2023:** the online course "Protecting Privacy and Access to City Records", which is mandatory for City Staff and provided to elected officials during the City's Privacy Awareness Week.
- **November 2023:** a mandatory session conducted by legal counsel and the Privacy Officer on "Privacy Obligations for Elected Officials".
- **May 2024:** an invitation extended to the Mayor to meet with the City's Privacy department and ask questions regarding his privacy obligations.
- **May 2024:** the online course "Protecting Privacy and Access to City Records", which is mandatory for City Staff and provided to elected officials during the City's Privacy Awareness Week.
- **December 2024:** the City's Privacy Officer emailed officials to remind them of their statutory duties under FIPPA.
- **June 2025:** the online course "Protecting Privacy and Access to City Records", which is mandatory for City Staff and provided to elected officials during the City's Privacy Awareness Week.
- **June 2026:** the online course "Protecting Privacy and Access to City Records", which is mandatory for City Staff and provided to elected officials during the City's Privacy Awareness Week.

[54] I also note that when the Mayor disclosed some of this same personal information on a previous occasion, the City sent him a letter on March 31, 2026, in which it advised that:

City records may not be released to the media or the public – whether in hard copy or electronic format (e.g. email or text message), or personally viewed – without the City's FOI staff and/or the CAO confirming they do not contain any confidential, in camera, personal, proprietary or other information that is legally protected from disclosure. For clarity, the expression "FOI-able" does not mean records are releasable, it means they can be requested, and there is a legislated FOI process to be followed.

[55] Based on the above, it is clear that the City has given its elected officials, and the Mayor in particular, an abundance of information and training opportunities on their duties imposed under FIPPA respecting personal information. Accordingly, the Mayor's decision to disclose personal information despite this can only be the result of willful ignorance or deliberate disregard of his duty under s. 25.1 of FIPPA not to disclose personal information except as authorized by this Act .

[56] In my view, the City has already exhausted all measures that could reasonably be expected to prevent further breaches of this nature.

FINDINGS

[57] I find that the Mayor disclosed the personal information of four individuals through the email and attachment he sent August 27, 2026 in contravention of s. 25.1 of FIPPA.

[58] I find that the City's response to the breach complied with s. 30 of FIPPA. Furthermore, because the City amended its notification to affected individuals on October 1, 2026, I find that the City has complied with s. 36.3 of FIPPA.

ORDERS

[59] I have carefully considered an appropriate remedy for the above findings. In general, the approach of the OIPC is remedial, with a focus on helping public bodies and individuals understand and comply with FIPPA. I note that the City reported to the OIPC privacy breaches by the Mayor on at least 35 separate occasions and the City made significant efforts to work with the Mayor and address his handling of personal information through remedial measures.

[60] Still, the City has reported to the OIPC that the Mayor has continued to disclose the personal information of City staff on multiple occasions during the course of this current investigation. The Mayor's repeated disclosure of personal information represents a flagrant disregard for the privacy of City staff and the duties imposed on him under FIPPA.

[61] It is significant that the Mayor's privacy breach on August 27, 2026 involved some of the same sensitive personal information he disclosed in March 2026, despite being advised that he lacked authority under FIPPA to disclose it. As previously noted, this leads me to conclude that this is the result of willful ignorance or deliberate disregard of FIPPA.

[62] For these reasons, it is evident that recommendations or voluntary remedies would be inadequate. Accordingly, I have decided to issue an order. Pursuant to ss. 58(3)(a) and 58(4) of FIPPA:

- a) I require Mayor Reid Hamer-Jackson to comply with his duty not to disclose personal information, including health information, obtained in the course of his duties as an officer of the City of Kamloops, except as authorized by FIPPA. As a condition of this order, the Mayor must receive written permission from the head of the public body, or their delegate, before disclosing any personal information of current or former municipal staff.

- b) I require Mayor Reid Hamer-Jackson to comply, by end of day on October 13, 2026, with the directions the City of Kamloops gave in the letter dated August 27, 2026, including the instruction to confirm in writing to the City the steps taken to comply.

[63] If Mayor Reid Hamer-Jackson does not comply with any of the above orders, the OIPC reserves the right under s. 59.01 of FIPPA to file the relevant order(s) with the Supreme Court.

October 9, 2026

ORIGINAL SIGNED BY

Ryan Graves
Investigator

OIPC Investigation No.: GEN-F-26-00714