



Order F26-65

SAANICH POLICE DEPARTMENT

Rene Kimmett
Adjudicator

July 22, 2026

CanLII Cite: 2026 BCIPC 80
Quicklaw Cite: [2026] B.C.I.P.C.D. No. 80

Summary: An individual (complainant) made a complaint that the Saanich Police Department (SPD) had used, disclosed, and failed to protect her personal information in violation of Part 3 of the *Freedom of Information and Protection of Privacy Act* (FIPPA). The adjudicator found the SPD had used and disclosed the complainant's personal information contrary to FIPPA. The adjudicator further found the SPD had failed to meet its obligations to protect the complainant's personal information and to adequately respond to her privacy breach complaint. The adjudicator ordered the SPD to stop the unauthorized use and disclosure of the complainant's personal information. The adjudicator also made recommendations for ways the SPD can improve its protection of personal information.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c. 165, ss. 25.1, 30, 32, and 33(1).

INTRODUCTION

[1] An individual (complainant) made a complaint that the Saanich Police Department (SPD) had used, disclosed, and failed to protect her personal information in violation of Part 3 of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

[2] The complainant took her concerns directly to the SPD, but it did not respond. She then made a complaint to the Office of the Information and Privacy Commissioner (OIPC). The OIPC's investigation did not resolve the matter, and it proceeded to this inquiry.

[3] The complainant, the SPD, and the police officer (Officer) involved in the alleged use and disclosure of the complainant's personal information were invited

to participate in this inquiry. The Officer declined to provide a submission on the basis that any submission in this inquiry may be prejudicial to his ongoing disciplinary proceedings before the Office of the Police Complaint Commissioner (OPCC).

ISSUES AND BURDEN OF PROOF

[4] In this inquiry, the issues are whether the SPD:

1. used the complainant's personal information contrary to s. 32;
2. disclosed the complainant's personal information contrary to s. 33;
3. made reasonable security arrangements to protect personal information as required by s. 30; and
4. took reasonable steps in response to a privacy breach as required by s. 30.

[5] Section 57 of FIPPA establishes the burden of proof in some types of inquiries but does not specify which party has the burden to prove the issues in dispute in this inquiry.

[6] Previous OIPC orders that deal with ss. 32 and 33 state that the public body will ordinarily be in the best position to prove its compliance with FIPPA and that each party must provide evidence and argument to support their position where the inquiry engages Part 3 of FIPPA.¹

[7] In Order F25-23, I found that, during an inquiry into whether a public body has collected a complainant's personal information contrary to s. 26, the public body has the burden to prove it complied with FIPPA by proving either that the collection did not occur or was authorized by FIPPA.²

[8] I find the burden of proof analysis under s. 26 is readily transferrable to ss. 30, 32, and 33 because the purpose, substance, and effect of these sections and the practical considerations affecting the burden of proof is similar. The purpose of these sections is to limit the circumstances in which a public body may use and disclose personal information in order to protect personal privacy. If a public body is alleged to have used, disclose, or failed to safeguard personal information contrary to FIPPA, it will, as a practical matter, need to raise a defence or be found in violation of FIPPA. Where a public body believes a use or disclosure has not occurred or that a use or disclosure was authorized by FIPPA,

¹ Order F25-01, 2025 BCIPC 1 (CanLII) at para 7.

² Order F25-23, 2025 BCIPC 28 (CanLII) at paras 20-33.

it has the expertise, knowledge, and resources to put forward arguments on the appropriate interpretation of FIPPA and its application to the relevant facts.

[9] Based on the above, I find that the SPD has the burden of proof under ss. 30, 32, and 33.

DISCUSSION

Factual findings

[10] Beginning in June 2022, the complainant had a dispute with another individual, which included the complainant making a criminal complaint against the individual. The Officer was assigned to files related to this ongoing dispute. The dispute was resolved in October 2023.³ The complainant filed several professional standards complaints about the Officer with the OPCC beginning in October 2023.

[11] In May 2023, the Officer told the complainant he was interested in pursuing a casual sexual relationship with her.⁴

[12] The complainant has included screenshots of text messages she says were sent to her from the Officer's personal cellphone in June 2023.⁵ The SPD submits "there is no independent way to verify the authenticity, accuracy, or completeness of the text messages referenced by the Complainant, nor to determine whether they reflect original, unaltered communications or the context in which they were exchanged."⁶

[13] There is no evidence before me that suggests the text messages the complainant has provided, as part of her affidavit evidence, are inauthentic, inaccurate, incomplete, altered or taken out of context. In the absence of evidence from the SPD or the Officer, both of which had the opportunity to participate in this inquiry, I find that the text messages the complainant has provided are accurate and unaltered and show the messages the Officer sent her from his personal cellphone in June 2023.

[14] I find the following excerpts from the text messages relevant to the issues in dispute in this inquiry:

Officer:	The situation is no I would not want my ex to ever find [out] about us [having sex]
----------	---

³ Complainant's affidavit #1 at paras 2-4.

⁴ *Ibid* at para 10.

⁵ *Ibid* at Exhibit B, PDF page 14.

⁶ SPD's submission at para 25.

[...]

That's rule 1 for me [...] anything between u and me stays here

[...]

Like if Saanich police found out I would never get promoted haha

Complainant: Why are you not with your ex?

[...]

Do you want her back?
I'm confused why she matters

Officer: We may or may not get back together one day.
Sleeping with [complainant's first and last name] won't help that. So [I] wouldn't risk her finding out while there's potential of a reconciliation.

Complainant: Do I know her
Does she know me?

Officer: "Anybody in my life knows of you [complainant's first name]!!!!
U tormented me for over a year! They might not know like who u are but knows of the [horror] associated to u

[...]

Complainant: Like, it would be sleeping with ME specifically that would be bad

Officer: Oh ya
Cuz I would give updates to all the drama
Like my mom would be blown away if she ever found out haha
People were invested "What's new with the file?"

Did the SPD use the complainant's personal information contrary to s. 32?

[15] A public body and its employees, officers or directors are permitted to use personal information if the use is authorized under FIPPA.⁷ Section 32 requires a public body to ensure that personal information in its custody or under its control is used only as specified under that section. Section 32 reads:

32 A public body may use personal information in its custody or under its control only

- (a) for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose,
- (b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or
- (c) for a purpose for which the information may be disclosed to the public body under section 33.

[16] A use is consistent with the purpose for which the information was obtained or compiled, under s. 32(a), if the use

- (a) has a reasonable and direct connection to that purpose, and
- (b) is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses [...] the information.⁸

[17] The SPD acknowledges it is responsible for ensuring personal information contained in its records is only used for an authorized police-related purpose.⁹ The SPD submits that the Officer was authorized to access the complainant's personal information to further the investigation of her file and there is no evidence of improper use of the complainant's personal information within the meaning of s. 32 of FIPPA.¹⁰

[18] The complainant submits the Officer used her personal information for casual personal reasons related to satisfying his friends' and family's curiosity about her police file.¹¹

[19] She submits s. 32(a) does not apply because her personal information was collected for the purpose of investigating a crime and using her personal

⁷ FIPPA, s. 25.1

⁸ FIPPA, s. 34.

⁹ SPD's submission at para 24.

¹⁰ *Ibid* at para 16.

¹¹ Complainant's initial submission at paras 34 and 35.

information to satisfy curiosity or personal interest is not consistent with the purpose of collection.

[20] The complainant submits she did not consent to her personal information being used for these purposes and, therefore, s. 32(b) does not apply.

[21] The complainant submits that none of the circumstances under s. 33 authorized disclosure of the personal information contained in her police file and, therefore, s. 32(c) does not apply.¹²

[22] I am satisfied that the complainant's police file contained recorded information about the complainant, who was identifiable from that record. As a result, I find the complainant's police file contained her personal information.¹³

[23] I find that the Officer used the complainant's personal information for the purpose of gossiping with his friends and family about her police file. As an example, when the complainant asked if the Officer's ex-partner knew who she was, the Officer replied by saying that "anybody in [his] life" knows of the "horror" associated with the complainant because he would give them updates about "all the drama" to the point that people were invested and asking "what's new with the file?"

[24] I find the use of the complainant's personal information to gossip is not authorized by s. 32(a). The complainant's personal information was obtained for the original purpose of investigating criminal allegations. There is no reasonable and direct connection between the purpose for obtaining the personal information, which was investigating a crime, and the Officer using the personal information to give his friends and family updates about "all the drama" associated with the complainant's file.¹⁴

[25] I agree with the SPD that the Officer was authorized to access the complainant's personal information for the purpose of furthering the criminal investigation. However, I am not persuaded by the SPD's assertion that there was no improper use of the complainant's personal information. The Officer's use of the complainant's personal information to gossip with his friends and family is an improper use and not authorized by s. 32(a) of FIPPA.

[26] I find the complainant did not consent, in any manner, to have her personal information used for the purpose of giving the Officer's friends and

¹² Complainant's initial submission at paras 37-39.

¹³ FIPPA, Schedule 1, definition of "personal information" and "contact information".

¹⁴ In reaching this conclusion, I have adopted the interpretation of "reasonable and direct connection" from Order F25-01, 2025 BCIPC 1 (CanLII) at para 64; see also "Investigation Report 00-01 Use of Alumni Personal Information by Universities", 2000 CanLII Docs 327.

family updates about her file and, therefore, this use was also not authorized under s. 32(b).

[27] The SPD does not say, and I cannot see how, s. 32(c) applies in the circumstances and I find that it does not.

Did the SPD disclose the complainant's personal information contrary to s. 33?

[28] A public body and its employees, officers or directors are permitted to disclose personal information if the disclosure is authorized under FIPPA.¹⁵ Section 33 requires a public body to ensure that personal information in its custody or under its control is disclosed only as specified under that section.

[29] I have already found that the complainant's police file contained her personal information because I am satisfied that it contained recorded information about the complainant, who was identifiable from that record. I have also found that the Officer verbally shared information from the complainant's police file with his friends and family.¹⁶

[30] Since information is only "personal information" if it is reasonably capable of identifying an individual, the last question I must answer is whether the information the Officer shared could reasonably be capable of identifying the complainant either by itself or when combined with other available sources of information.¹⁷

[31] The SPD submits that there is insufficient evidence to establish that a disclosure occurred. It submits that the complainant did not provide any supporting affidavits, from the Officer's friends or family, alleging a disclosure occurred.¹⁸ It submits that the complainant relies on a limited set of text messages that do not, on their face, establish that there was a disclosure of personal information obtained through police databases. The SPD submits that the Officer clearly wanted his personal relationship with the complainant to be kept secret, particularly from his mother and ex-partner, and, therefore,

common sense would dictate that the [Officer] had a vested interest in not disclosing any personal information that would identify the Complainant. [...] it is unlikely that the [Officer] would disclose the Complainant's

¹⁵ FIPPA, s. 25.1

¹⁶ In Order F14-26, the adjudicator concluded "verbally communicated information about an identifiable individual is 'personal information' as long as it exists or existed at one time in recorded format." Order F14-26, 2014 BCIPC 29 (CanLII) at para 16.

¹⁷ Order F05-30, 2005 CanLII 32547 (BC IPC) at para 35.

¹⁸ SPD's submission at para 20.

personal information to others, especially when he clearly wanted this relationship to remain a secret.¹⁹

[32] The complainant says that the texts support her position that there was an unauthorized disclosure by the Officer to individuals outside of those tasked with investigating her criminal complaint. She says she is concerned that the disclosure may have included her name and other identifying information.²⁰ She submits that many individuals could reasonably be expected to identify her from the context of her police file because, at the time, she worked in close proximity to the SPD's building and played on a sports team with members of the Officer's social and professional circles.²¹

[33] For the reasons below, I find, on a balance of probabilities, that the verbally shared information was reasonably capable of identifying the complainant and, as a result, find the Officer disclosed the complainant's personal information.

[34] The SPD says that, to prove there was an unauthorized disclosure, the complainant should have provided affidavit evidence from the Officer's friends and family.²² However, the SPD, not the complainant, has the burden of proof in this inquiry.

[35] The SPD submits the Officer must not have disclosed personal information contained in the complainant's police file because he clearly did not want to disclose information about their sexual relationship. I reject this argument. I find the text messages indicate that the Officer did not want to tell his friends and family about his sexual relationship with the complainant because he had already used the complainant's personal information to gossip with his friends and family about her file. The texts do not provide evidence to support the SPD's position that the Officer did not disclose the complainant's personal information.

[36] In the texts, the Officer says that his friends and family "might" not know who she is, leaving open the possibility that they do know who she is. Further, the texts indicate that the Officer had been giving detailed and ongoing updates

¹⁹ SPD's submission at para 21.

²⁰ Complainant's affidavit #1 at para 18.

²¹ *Ibid* at para 9.

²² For the complainant to provide affidavit from the Officer's friends or family, she would have needed to know the names and contact information of these individuals. The process of getting these affidavits would have also required the complainant to confirm to these individuals that she was the person the Officer had been gossiping about. Lastly, as the friends and family of the Officer, these individuals may have been unwilling to provide evidence to the complainant supporting her claim that he had disclosed her personal information. It would be unreasonable and impractical to expect the complainant to provide this kind of evidence to support her complaint.

to his friends and family about her police file, which increases the likelihood that he shared identifying information about the complainant with people in his personal life.

[37] The SPD is responsible for complying with FIPPA. The SPD, as the public body and the Officer's employer, was in the best position, and indeed had an obligation under s. 30, to investigate the complainant's concerns about a privacy breach. The SPD's defence to the complainant's allegation of unauthorized disclosure is that a disclosure did not occur. However, as I discuss in more detail below, the SPD did not investigate the complainant's concerns and, as a result, does not have sufficient evidence to support its assertion that a disclosure did not occur.

[38] Based on the evidence before me, I find the SPD has not met its burden to prove, on a balance of probabilities, that a disclosure of the complainant's personal information did not occur.

[39] The SPD has also not made any arguments that the disclosure was authorized under s. 33. Without any submissions or evidence from the SPD on this point, I find the disclosure of the complainant's personal information was not authorized under FIPPA.

Did the SPD make reasonable security arrangements to protect personal information as required by s. 30?

[40] Section 30 requires public bodies to protect personal information in their custody or under their control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. Reasonable security arrangements include training, privacy policies, and confidentiality agreements. I address these arrangements under the subheadings below.

Training

[41] Training is a key part of making reasonable security arrangements under s. 30. Training is necessary for employees to understand the need for privacy and confidentiality, their legal and professional obligations, the processes put in place to protect privacy, and the consequences for failing to adhere to privacy obligations.²³

[42] The SPD submits that, when joining SPD, all police officers are required to complete a mandatory access and privacy training session with the SPD's Information and Privacy Coordinator (Coordinator). The SPD also submits that

²³ *Privacy breaches following the Lapu Lapu Day Festival*, 2026 BCIPC 10 (CanLII) at page 21. [Lapu Lapu Report].

the Coordinator periodically attends police officer meetings to remind SPD employees of their privacy obligations.²⁴

[43] The SPD has not provided any details about the content of this training session or the reminders about privacy obligations. While I do not know the content of the SPD's privacy training, the SPD's submissions in this inquiry and response to the complainant's privacy complaint leave me with concerns about the substance of this training.

[44] The SPD's submissions in this inquiry were made by the Coordinator. These submissions conflate access to personal information and use of personal information. The SPD argued that since the Officer accessed the complainant's personal information for legitimate policing purposes that he could not have subsequently used her personal information for unauthorized purposes. It maintained this position despite the clear evidence of the Officer contemporaneously admitting to the complainant that he had used her personal information to gossip with his friends and family about her police file. The SPD's submissions demonstrate a fundamental misapprehension about the difference between access to and use of personal information and the requirement that the SPD protect personal information not only from unauthorized access but also unauthorized use and disclosure.

Privacy policies

[45] Having a privacy policy is a key part of a public body's reasonable security safeguards under s. 30. The policy should make clear to public body employees what the rules and expectations are for handling personal information and how they work in practice. This includes potential consequences for when those rules are not followed.²⁵

[46] The SPD provided its policy on police database access (Access Policy).²⁶ The Access Policy sets out that no employee will access or use personal information in police databases for personal reasons or gain. It clearly states that access to personal information must be related to the legitimate performance of an employee's duties and that employees are expected to consult their supervisors if they are uncertain whether access is authorized.

[47] However, the Access Policy does not say that contravening the SPD's privacy policies will result in discipline. It also does not say that discussing personal information obtained or accessed for work purposes with people in their personal lives constitutes an unauthorized use of personal information and may also constitute an unauthorized disclosure if identifying information is shared.

²⁴ SPD's submission at paras 8-9.

²⁵ *Lapu Lapu Report*, *supra* note 23 at page 22.

²⁶ Information and Privacy Coordinator affidavit #1 at Exhibit 2.

Confidentiality agreements

[48] Confidentiality agreements or undertakings require employees to commit, in writing, to their privacy and confidentiality obligations. These agreements make those obligations clear and are important for holding employees accountable for their actions.²⁷

[49] The SPD has not said whether it requires its employees to sign confidentiality agreements or undertakings.

Privacy notices

[50] Privacy notices and flags remind employees that the personal information in a system can only be viewed for a legitimate purpose. They also can require employees to confirm there is a legitimate purpose for accessing records before they access the records.²⁸

[51] The SPD submits its computer system requires employees to agree with an “access acknowledgement” before accessing their computer. It reads as follows:

By clicking the "OK" button you agree that you are accessing the confidential database of the Saanich Police Department in the lawful execution of your duties and/or for a valid police purpose. Accessing SPD databases for any other reason is a violation of [the Access Policy].

[52] While this privacy notice serves an important function, it is not a safeguard against unauthorized use or disclosure and instead only addresses the issue of access to personal information.

Privacy breach management

[53] An established breach management process enables public bodies to respond more effectively to the unauthorized collection, use or disclosure of personal information. This management is critical to safeguarding personal information in terms of the timeliness and efficacy of the breach response.²⁹

[54] The SPD also provided its policy on privacy breaches (Breach Policy). The Breach Policy contains useful information about how the SPD will respond to privacy breaches. However, it does not contain FIPPA’s definition of privacy breach and does not include the 2021 amendments to FIPPA that specify when privacy breach notification and reporting is required. It also does not explain how the SPD will respond to unconfirmed allegations of privacy breaches. As written,

²⁷ *Lapu Lapu Report*, *supra* note 23 at page 22.

²⁸ *Ibid* at page 23.

²⁹ *Ibid* at page 25.

the Breach Policy only deals with the SPD's responses to actual privacy breaches and not alleged or suspected privacy breaches.

Did the SPD take reasonable steps in response to the complainant's alleged privacy breach as required by s. 30?

[55] Another requirement under s. 30 is that public bodies take reasonable steps to respond to privacy breaches.

[56] I am satisfied the complainant brought her concerns about a possible privacy breach to the SPD. For the reasons below, I find the SPD did not take reasonable steps to respond to those concerns.

[57] The OIPC has published a guidance document that sets out four steps for responding to privacy breaches in a manner that is consistent with s. 30.³⁰ The OIPC considers each step in determining whether a public body's response to a breach met its duty to safeguard personal information. These steps include containment, risk assessment, notification (as applicable) and prevention.

[58] The first step is to take immediate, common-sense steps to limit the privacy breach by, for example, immediately stopping the unauthorized practice. An appropriate individual should conduct an initial investigation and, if necessary, a more detailed investigation may subsequently be required.

[59] The second step involves immediately assessing the cause and extent of the breach and the potential harm to individuals, the public, and the public body resulting from the breach.

[60] The third step involves immediately assessing whether it is appropriate or mandatory to notify affected individuals. Subject to some exceptions, a public body must notify affected individuals and the OIPC, if the unauthorized use or disclosure could reasonably be expected to result in significant harm to the individual, including humiliation or damage to reputation or relationships.

[61] The fourth step is to thoroughly investigate the cause of the breach and determine whether any safeguards need to be developed or improved to prevent further breaches.

[62] The SPD submits that a privacy breach did not occur or, in the alternative, if it did occur, that the SPD complied with its Breach Policy because it notified the OPCC, preserved relevant records, and deferred to independent oversight (by which I believe it means the OPCC) to assess the allegations.³¹

³⁰ *Privacy breaches: tools and resources for public bodies*, online: <https://www.oipc.bc.ca/documents/guidance-documents/2584>.

³¹ SPD's submission at paras 7 and 12.

[63] I have already found in this order that a privacy breach did occur because the Officer used and disclosed the complainant's personal information for an unauthorized purpose.

[64] Respectfully, I find the SPD did not follow its Breach Policy. This policy says the SPD will assess the potential risk to individuals, determine whether to notify affected individuals, and determine whether changes need to be made to prevent similar future privacy breaches.³² There is no evidence before me that the SPD took any of these steps. Further, the evidence before me, which the SPD has not contradicted, is that it did not even reply to the complainant's letter in which she raised her concerns about the unauthorized use and disclosure of her personal information.

[65] The SPD cannot delegate its responsibilities under FIPPA to the OPCC. The SPD, as the public body with custody and control of the complainant's personal information, has the responsibility to protect that information. This responsibility includes responding appropriately to her concerns about unauthorized use and disclosure. The obligation to ensure employees are safeguarding personal information continues to rest with the public body employer, even where its employees may be subject to additional oversight by a professional regulatory body, such as the OPCC.

Conclusion – s. 30

[66] For the reasons above, I find that together, the SPD's privacy policies, practices, and training are not reasonable security arrangements against unauthorized use or disclosure of personal information and that the SPD did not reasonably respond to the complainant's concerns about the use and disclosure of her personal information.

Remedy

[67] On completing an inquiry under s. 56, I must dispose of the issues by making an order under s. 58. Section 58(3)(e) is the subsection relevant here and it reads:

(3) If the inquiry is into any other matter, the commissioner may, by order, do one or more of the following:

[...]

(e) require a public body or service provider to stop collecting, using or disclosing personal information in contravention of

³² Information and Privacy Coordinator affidavit #1 at Exhibit 3.

this Act, or confirm a decision of a public body or service provider to collect, use or disclose personal information;

[68] I found the SPD's use of the complainant's personal information was not authorized under s. 32 and its disclosure of the complainant's personal information was not authorized under s. 33. As a result, the only remedy available for these contraventions of FIPPA is an order under s. 58(3)(e) requiring the SPD to stop its unauthorized use and disclosure of the complainant's personal information.

[69] However, I have also found the SPD's safeguards against unauthorized use and disclosure of personal information, including its response to the complainant's allegations of unauthorized use and disclosure, to be significantly lacking. As a result, I recommend the SPD update its privacy policies, training, and practices after consulting with a privacy expert. Updates the SPD may wish to consider include:

- conducting privacy training on an annual basis;
- communicating to staff, through training and policies, that using personal information to discuss a police file with individuals not involved with the file constitutes an unauthorized use of personal information and may constitute an unauthorized disclosure if identifying information is shared;
- developing disciplinary guidelines that are strong enough to effectively deter unauthorized access, collection, use, disclosure, and disposal of personal information;
- requiring staff to sign confidentiality agreements;
- adding FIPPA's definition of "privacy breach" to its privacy training and policies;
- adding FIPPA's mandatory notification and reporting requirements to its privacy training and policies;
- clarifying that its privacy policies apply not only to confirmed privacy breaches, but also alleged or suspected privacy breaches; and
- clarifying that reporting a privacy breach or complaint to the OPCC, or other regulatory authority, does not replace the SPD's responsibilities to appropriately respond to the privacy breach or complaint.

CONCLUSION

[70] For the reasons given above, I find the SPD's use of the complainant's personal information was not authorized under s. 32 and its disclosure of the complainant's personal information was not authorized under s. 33. Accordingly, under s. 58(3)(e) of FIPPA, I make the following order: I require the SPD to stop using and disclosing the complainant's personal information in contravention of ss. 32 and 33 of FIPPA.

[71] I also strongly encourage the SPD to improve its privacy policies, training, and practices by, for example, implementing the recommendation I have made above.

July 22, 2026

ORIGINAL SIGNED BY

Rene Kimmett, Adjudicator

OIPC File No.: F24-98378