

March 12, 2026

Gabriola Fire Protection Improvement District
e. corporateofficer@gabriolafire.ca

Dear Marjorie Colebrook:

**Re: Breach Notification - Improper Disposal
Gabriola Fire Protection Improvement District
OIPC File: PRI-F-25-00461**

I am the Investigator assigned to complete the monitoring of the privacy breach reported to this office on October 13, 2025.

This report is made pursuant to s. 42 of the *Freedom of Information and Protection of Privacy Act* (FIPPA). This report examines the adequacy of protective measures taken by the Gabriola Fire Protection Improvement District (the public body) under s. 30 of FIPPA. This report makes findings and contains conclusions, but no order is made under s. 58 of FIPPA.

Incident Description

The Chair of the Board for the public body received a computer (delivered by a community member), previously owned by the public body. The device was disposed of approximately three years ago (2022-2023) as part of an equipment replacement cycle.

In the wake of discussions about records management practices at the public body, the community member recognized the device they had possession of appeared to contain sensitive personal information, and they turned the computer over to the public body.

The personal information was stored locally on the computer in question, and the computer was not connected to the internet for any extended period. The public body has confirmed that the personal information contained on the computer was:

- Names
- Email Addresses (pre-2015)
- SINS

Protection of Personal Information

Public bodies in British Columbia are under a statutory duty to protect the personal information in their custody or under their control. Section 30 of FIPPA sets out the legal requirement:

30 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 in s. 30 of FIPPA has been examined in a number of orders. In paragraph 75 of order F15-57¹, 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.*”

Response to the Privacy Breach

To assist public bodies in evaluating their compliance with the reasonable security standard, this office has described four key steps for managing a privacy breach. When a privacy breach occurs, public bodies must make every reasonable effort to contain the breach, recover the personal information, minimize the harm resulting from the breach and prevent future breaches from occurring. It is in this context that I have reviewed and evaluated the actions of the public body in response to this privacy breach.

1. Breach Containment

Containment mitigates the impact of the breach by limiting further dissemination of the personal information at issue. This breach was discovered when a community member realized potentially sensitive information, belonging to the public body, was retained on a computer they possessed.

All the information on the computer was stored locally, and was not connected to a public server, or the internet. Once the breach was discovered, the computer was returned to the public body. The computer was then securely stored at the public body. Furthermore, the public body has stated:

At the request of the Chair Erik Johnson, Trustee David Chorneyko negotiated a statement from the person(s) who removed the computer from the Hall, but wished to remain anonymous, that the computer had been solely in this persons possession for three years and they had not shared information with anyone as to the file contents of the computer and it’s hard drive. Then Chair Wayne Mercier took possession of the computer tower from the person who had it for the past three years on Friday, October 10, 2025 and returned it to the current Corporate Officer on

¹ [OIPC Order F15-57](#)

October 22, 2025. It was stored under lock and key and not accessed by anyone after it was returned by Trustee Mercier.

In my view, this breach was appropriately contained.

2. Risk of Significant Harm

To determine what additional steps are immediately necessary, public bodies are required to evaluate the risks associated with the breach. This includes determining whether the privacy breach could reasonably be expected to result in one or more of the significant harms listed in s. 36.3(2)(a) of FIPPA.

The public body reviewed the information stored on the computer. Although the computer was the main public body computer from 1996 to 2015, there was little information on it. Most of the data appeared to have been deleted when transferred. Unfortunately, some personal information about firefighters who worked at the public body from 1996-2015) remained.

The public body specifically wrote:

We identified 57 individuals who had information on that computer. We were able to find all SIN numbers on file and their corresponding Firefighters. This will allow us to individually notify each firefighter whose SIN was on the hard drive that their personnel data was breached.

The public body also confirmed that the data was only accessed by the community member who possessed the computer, and the previous chair of the public body.

Furthermore, the public body did not find any new inputs in the hard drive (where the breached personal information was stored), apart from three files that were created on the desktop of the computer, during this investigation.

In my view, there is not a risk of significant harm, as it does not appear this data was accessed in any malicious way, and when it was discovered by the community member, it was returned to the public body. However, due to the nature of the information breached, and in keeping with the public body's commitment to transparency, and improving their records procedures, notification in this instance is something I would recommend, although, it doesn't necessarily meet the mandatory threshold under s. 36.3(2) of FIPPA.

3. Notification

The public body notified affected individuals in January 2026, via mail. I have reviewed the anonymized notification, and in my view it complies with section 36.3 of FIPPA and contains the relevant information as outlined in the FIPPA Regulation.

Within the notification, the public body offered complimentary credit monitoring to affected individuals.

Additionally, the public body put an add out in the local newspaper, notifying the public of the breach, and asking anybody who was a firefighter from 1996-2015, and did not receive a notification (due to potentially outdated contact information), to contact the public body.

4. Prevention Strategies

Records management has been identified as an issue at the public body, that they are now addressing. The public body has identified a few immediate prevention and mitigation steps:

- Credit monitoring for affected individuals
- Securing records from the breached computer and bringing them in line with records management practices of the public body.

The above strategies are a great place to start. I understand from speaking with the public body, that they are working on re-vamping their records processes, and are formalizing administrative responsibilities, so that going forward, they can improve their records practices. I am satisfied that the public body is taking this matter seriously.

The public body has asked the OIPC for guidance on what to do with the information found on the computer. I cannot give you a specific answer, but the public body will need to review the information, and any applicable retention schedules for information (for example, financial information has a different retention schedule than email correspondence). The public body should then retain information securely based on those schedules, and any applicable internal policies, or bylaws (and of course in conjunction with FIPPA). My recommendation for overall records management, would be to first take stock of the type of records the public body keeps, and create practices and schedules for each type of record. This can sound daunting, but, in my view, the administrative organization will assist the public body's operations to move more smoothly in the future.

Furthermore, I have linked some OIPC resources below, our office also has an educational mandate, and we are here to answer questions, should any arise in the future.

- “Securing Personal Information: A Self-Assessment Tool for Public Bodies and Organizations”: <https://www.oipc.bc.ca/resources/breach-notification-representatives-of-organizations-and-public-bodies/>
- “Accountable Privacy Management in BC’s Public Sector”: <https://www.oipc.bc.ca/documents/guidance-documents/1468>
- General resources: <https://www.oipc.bc.ca/for-public-bodies/>

After reviewing the actions taken by the Gabriola Fire Protection Improvement District, I am satisfied that it has taken reasonable steps to respond to this breach.

This concludes the monitoring of this privacy breach, and the above referenced file has been closed. If you have any questions, please contact me at 250-896-2035 or tlaughlin@oipc.bc.ca.

Sincerely,

A handwritten signature in cursive script that reads "Tara Laughlin".

Tara Laughlin
Investigator