Fraser Valley Regional District

Issued	March 2023
Amended	

PRIVACY BREACH POLICY

PURPOSE AND INTENT

The Fraser Valley Regional District Privacy Breach Policy sets out the legal obligations of the organization with respect to compliance and accountability with respect to privacy breaches pursuant to the *Freedom of Information and Protection of Privacy Act* ("FOIPPA").

This policy is intended to support the Fraser Valley Regional District's ("FVRD") Privacy Management Program, and to demonstrate the FVRD's commitment to protecting privacy and personal information in its day-to-day business operations through responsible privacy management practices, and ensuring compliance with FOIPPA.

PRINCIPLES

The FVRD recognizes that the need to collect, use or disclose personal information for the purpose of carrying out its operations must be balanced against the right of individuals to have their privacy and personal information protected.

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information pursuant to FOIPPA. A privacy complaint is a complaint from an individual about a breach of their own personal information.

The FVRD commits to taking reasonable security precautions to protect against a privacy breach through unauthorized access to or collection, use or disclosure of personal information.

The FVRD commits to the following four key steps regarding compliance with FOIPPA:

1. Reporting and Containment of the Privacy Breach

All privacy breaches and complaints regarding suspected privacy breaches must be immediately reported to the Privacy Officer as soon as they become known. The Privacy Officer will take immediate steps to contain and manage the privacy breach.

The Privacy Officer is responsible for the conduct of privacy breach investigations and where required will involve members of an Investigation Team.

2. Risk Evaluation

The Privacy Officer will conduct a risk evaluation to determine the personal information involved, including the cause and extent, what individuals may be affected, and the foreseeable harm from the privacy breach. The Privacy Officer will also determine whether affected individuals should be notified.

3. Notification

If notification is required, the Privacy Officer will consider if the affected individuals are required to be notified, and what should be included in the notification. Notification will be in accordance with FOIPPA and will occur as soon as possible following a Privacy Breach.

4. Prevention

Once the Privacy Officer has taken immediate steps to mitigate the risks associated with the Privacy Breach, the Privacy Officer will thoroughly investigate the cause of the Privacy Breach.

The Privacy Officer will determine whether any improvements or changes to security safeguards are needed as a result of the Privacy Breach.

DEFINITIONS

"Office of the Information and Privacy Commissioner" provides independent oversight and enforcement of BC's access and privacy laws, including FOIPPA, which applies to Public Bodies.

"*Privacy Breach"* means the unauthorized collection, use and disclosure of personal information in the course of FVRD business.

"Personal Information", broadly defined, means recorded information, other than contact information, about an identifiable individual, including, but not limited to, the following:

- The individual's name, address or telephone number;
- The individual's race, national or ethnic origin, colour, religious or political beliefs or associations;
- The individual's age, sex, sexual orientation, marital status or family status;
- An identifying number, symbol or other particular assigned to an individual;
- The individual's fingerprint, blood type or inheritable characteristic;
- Information about the individual's health care history, including a physical or mental disability;
- Information about the individual's education, financial, criminal or employment history;
- Anyone else's opinion about the individual (but not the identity of the opinion holder); or
- The individual's personal view or opinion, except if they are about someone else (you can know what is said about you but you cannot necessarily know who said it).

"Privacy Officer" means the person, or persons designated by the FVRD Board, who is responsible for the administration of the FVRD Privacy Management Program.

"Public Body" means a local government body.

APPLICATION AND ACCOUNTABILITY

The FVRD is a deemed Public Body under FOIPPA and has a statutory obligation to protect privacy and Personal Information from unauthorized collection, use and disclosure.

This Privacy Breach Policy applies to all FVRD employees, Board Directors, agents, volunteers, and service providers, and sets out the expectations and obligations to report Privacy Breaches when they happen, the reporting process, managing Privacy Breaches, assigning responsibility for investigating Privacy Breaches and subsequent follow up pursuant to FOIPPA.

All FVRD employees, Board Members, agents, volunteers, and service providers are responsible for:

- Complying with this policy;
- Consulting with the Privacy Officer regarding the requirements of FOIPPA and this policy; and
- Immediately reporting suspected or confirmed Privacy Breaches to the Privacy Officer.

No person shall collect, use or disclose any Personal Information except in accordance with FVRD policies and FOIPPA.

As required, the Privacy Officer, or their delegate, may carry out a Privacy Breach investigation and may collect, use and disclose Personal Information for the purpose of conducting the investigation.

Where a Privacy Breach involves an employee and an investigation is to take place, the Human Resources and Information Technology Departments may be engaged in the investigation. Privacy Breach investigations will be confidential.

After the investigation is completed, a written report will be prepared by the Privacy Officer. The report will contain findings of fact and recommendations aimed at ensuring compliance with this policy and FOIPPA.

POLICY AND PROCEDURE: PRIVACY BREACHES

Privacy Breaches may be identified through any one of the following ways:

- Responding to a Personal Information usage or privacy complaint;
- Monitoring systems in FVRD facilities;
- Responding to an Privacy Breach; or
- Reporting from an external source.

Any employees, agents, volunteers or service providers who are made aware of any Privacy Breach must immediately notify their direct supervisor. The supervisor will report the Privacy Breach to the Privacy Officer.

Any Board Directors who are made aware of any Privacy Breach must immediately notify the Privacy Officer.

If an Investigation Team is required, the Privacy Officer will determine which FVRD employees to designate for the investigation, assessment and resolution of the Privacy Breach.

The Privacy Officer has oversight of any Investigation Team necessary for the assessment and resolution of each specific Privacy Breach.

The Privacy Officer and, if necessary, Investigation Team will:

- Conduct an assessment to determine the nature and scope of the Privacy Breach;

- Take actions to immediately contain the Privacy Breach;
- Complete the Privacy Breach checklist (refer to the OIPC "Privacy Breach Checklist" attached as Appendix A to this policy); and
- Conduct a risk assessment;
- Produce reports and assessment records that will be maintained by the Privacy Officer;
- Determine the communications necessary and the internal and external reporting requirements;
- Complete a Breach Notification Assessment and determine the notifications necessary and produce such notifications (refer to the OIPC "Breach Notification Assessment Tool" attached as Appendix B to this policy);
- Ensure that FVRD's business practices are improved where necessary to prevent similar future incidents;
- Take any other actions that arise from specific incidents as set out in the below Action Plan;
- Finalize the process with the conclusion of the internal and external reporting.

In the event of a Privacy Breach, and considering the nature of the breach, the Privacy Officer will assign the action steps below to the recommended personnel, as appropriate:

	Action Required	**Responsibility**	**Recommended Timelines**
1	Contain the breach	Affected department	Immediate
2	Report the breach within FVRD	Employee/agent/volunteer/service provider reports to Supervisor; Supervisor reports to Privacy Officer Board Director reports to Privacy Officer	Day of breach discovery
3	Designate Investigation Team as appropriate	Privacy Officer to chair Investigation Team and lead investigation	Day of breach discovery
4	Protect and preserve the evidence	Privacy Officer, affected department and Manager of Information Technology, GIS & FDM	Day of breach discovery
5	Contact RCMP if necessary	Privacy Officer	Day of breach discovery
6	Conduct preliminary analysis of risks and cause of breach	Privacy Officer and Manager of Information Technology, GIS & FDM	Within two days of breach
7	Determine whether to report the breach to affected individuals and/or the BC Privacy Commissioner	Privacy Officer	Within two days of breach
8	Take further containment steps as indicated by preliminary analysis	Privacy Officer and Manager of Information Technology, GIS & FDM	Within two days of breach
9	Evaluate risks associated with breach	Privacy Officer and Manager of Information Technology, GIS & FDM	Within one week of breach
11	Notify affected individual(s) as determined as per legislative requirements	Privacy Officer and Manager of Communications	Within one week of breach

12	Contact other parties as appropriate	Privacy Officer and Manager of Communications	As needed
13	Determine whether further, in-depth investigation is needed	Privacy Officer	Within two weeks of breach
14	Further investigate the cause and extent of breach if necessary	Privacy Officer and Manager of Information Technology, GIS & FDM	Within two weeks of breach
15	Review investigation findings and develop prevention strategies	Privacy Officer and Manager of Information Technology, GIS & FDM	Within three weeks of breach
16	Implement prevention strategies/improvements	Privacy Officer and Manager of Information Technology, GIS & FDM	Dependent on prevention strategy
17	Monitor prevention strategies	Privacy Officer and Manager of Information Technology, GIS & FDM	Privacy and security audits annually or as scheduled
18	Produce internal and external reports	Privacy Officer	After investigations and mitigation is completed

Reporting of Privacy Breach

The Privacy Officer will determine when reporting to the OIPC is required as per requirements under FOIPPA and associated regulations.

Appendix A: OIPC Privacy Breach Checklist
Appendix B: OIPC Breach Notification Assessment Tool

Step 1: Notifying affected individuals

Use this chart to help you decide whether you should notify affected individuals. If either of the first two factors listed below applies, notification of the individuals affected must occur. The risk factors that follow are intended to serve as a guide. If none of these applies, no notification may be required. You must use your judgment to evaluate the need for notification of individuals.

Consideration	Check if applicable
Legislation requires notification Are you or your organization covered by legislation that requires notification of the affected individual? If you are uncertain, contact the Privacy Commissioner (see contact information at the end of this publication).	☐
Contractual obligations Do you or your organization have a contractual obligation to notify affected individuals in the case of a data loss or privacy breach?	☐
Risk of identity theft Is there a risk of identity theft? How reasonable is the risk? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with password information and any other information that can be used for fraud by third parties (e.g. financial).	☐
Risk of physical harm Does the loss of information place any individual at risk of physical harm, stalking or harassment?	☐
Risk of hurt, humiliation, damage to reputation Could the loss of information lead to hurt, humiliation or damage to an individual's reputation? This type of harm can occur with the loss of information such as mental health records, medical records or disciplinary records.	☐
Loss of business or employment opportunities Could the loss of information result in damage to the reputation to an individual, affecting business or employment opportunities?	☐

Step 2: When and how to notify affected individuals

When:
Notification should occur as soon as possible following a breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.
How:
The preferred method of notification is direct – by phone, letter or in person – to affected individuals. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

The chart below sets out factors to consider in deciding how to notify the affected individuals.

Considerations favouring direct notification of affected individuals	Check if applicable
The identities of the individuals are known.	☐
Current contact information for the affected individuals is available.	☐
Individuals affected by the breach require detailed information in order to properly protect themselves from the harm arising from the breach.	☐
Individuals affected by the breach may have difficulty understanding	☐

Considerations favouring indirect notification of individuals	Check if applicable
A very large number of individuals are affected by the breach such that direct notification could be impractical.	☐
Direct notification could compound the harm to the individual resulting from the breach.	☐

Step 3: What to include in the notification of affected individuals

The information in the notice should help the individual to reduce or prevent the harm that could be caused by the breach. Include the information set out below:

Information required	Check information included
Date of the breach.	☐
Description of the breach. A general description of what happened.	☐
Description of the information. Describe the information inappropriately accessed, collected, used or disclosed.	☐
Steps the individual can take. Provide information about how individuals can protect themselves, e.g. how to contact credit reporting agencies (to set up credit watch), information explaining how to change a personal health number or driver's licence number.	☐
Privacy Commissioner contact information. Include information about how to complain to the Privacy Commissioner.	☐
Organization contact information for further assistance. Contact information for someone within your organization who can provide additional information and assistance and answer questions.	☐

Step 4: Others to contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach. Do not share personal information with these other entities unless required.

Authority or organization	Purpose of contacting	Check if applicable
Law Enforcement	If theft or other crime is suspected. (Note: The police may request a temporary delay in notifying individuals, for investigative purposes.)	☐
Office of the Information and Privacy Commissioner **250-387-5629** **info@oipc.bc.ca** oipc.bc.ca	For assistance with developing a procedure for responding to the privacy breach, including notification. To ensure steps taken comply with the organization's obligations under privacy legislation.	☐
Professional or regulatory Bodies	If professional or regulatory standards require notification of the regulatory or professional body.	☐
Technology suppliers	If the breach was due to a technical failure and a recall or technical fix is required.	☐

Privacy Breach Checklist for Public Bodies

Use this form to evaluate your public body's response to a privacy breach. The form can also be submitted to the OIPC for the purpose of mandatory notification, as it includes fields for all of the information required under the *Freedom of Information and Protection of Privacy Act*. If you are reporting the breach to the OIPC through the checklist or the online form, you must answer all of the questions. If a question does not apply to your situation, write "N/A." If you do not know the answer, write "unknown." Completed forms can be emailed to info@oipc.bc.ca

The preferred method for public bodies to report privacy breaches is by using our online form: https://www.oipc.bc.ca/forms/public-bodies/online-privacy-breach-report-form/

Information entered into the online form is secured through encryption in transit and storage.

For more information on reporting a privacy breach, visit:
https://www.oipc.bc.ca/resources/report-a-privacy-breach/

Contact information

Public Body:

Contact Person:

Name:

Preferred pronoun:

Title:

Phone:

Email:

Mailing address:

Risk evaluation

Incident Description

1. Describe the breach and its cause:

2. Date of the breach or period when it occurred:

3. Date breach discovered:

4. Location of breach:

5. Estimated number of individuals affected:

6. Type of individuals affected:

- ☐ Client/Customer/Patient
- ☐ Employee
- ☐ Student
- ☐ Other:

Personal Information Involved

7. Describe the personal information involved (e.g. name, address, SIN, financial, medical): (Do not include or send us identifiable personal information)

Safeguards

8. Describe physical security measures (locks, alarm systems etc.):

9. Describe technical security measures:

- ☐ Encryption
- ☐ Password
- ☐ Other (Describe):

Describe organizational security measures (security clearances, policies, role-based access, training programs, contractual provisions):

Harm from the Breach

10. Identify the type of harm(s) that may result from the breach:

- ☐ Identity theft (most likely when the breach includes loss of SIN, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with password information and any other information that can be used to commit financial fraud) or significant:
  - ☐ Bodily harm (when the loss of information places any individual at risk of physical harm, stalking or harassment);
  - ☐ Humiliation (associated with the loss of information such as medical records, disciplinary records);
  - ☐ Damage to reputation or relationships;
  - ☐ Loss of employment, business or professional opportunities (usually as a result of damage to reputation to an individual);
  - ☐ Financial loss;
  - ☐ Negative impact on a credit record, or;
  - ☐ Damage to, or loss of, property;
- ☐ Breach of contractual obligations;
- ☐ Future breaches due to similar technical failures;
- ☐ Failure to meet professional or certification standards;
- ☐ Other (specify): ☐

Notification

11. Has your Privacy Officer been notified?

☐ Yes Who was notified and when? _____

☐ No When to be notified? _____

12. Have the police or other authorities been notified (e.g. professional bodies or persons required under contract)?

☐ Yes Who was notified and when? _____

☐ No When to be notified? _____

13. Have affected individuals been notified?

☐ Yes Manner of notification: _____
Number of individuals notified: _____
Date of notification: _____

☐ No Why not? _____

14. What information was included in the notification?

☐ The name of the public body;

☐ The date on which the privacy breach came to the attention of the public body;

☐ A description of the privacy breach including, if known,

- ☐ (a) the date on which or the period during which the privacy breach occurred, and;
- ☐ (b) a description of the nature of the personal information involved in the privacy breach;

☐ Confirmation that the Commissioner has been or will be notified of the privacy breach;

- ☐ Contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;

- ☐ A description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;

- ☐ A description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

Notifying the OIPC

15. The Office of the Information and Privacy Commissioner must be notified of the breach if the breach could reasonably be expected to result in significant harm to the individual, including any of the harms listed below:

- ☐ Identity theft or significant
    - ☐ Bodily harm;
    - ☐ Humiliation;
    - ☐ Damage to reputation or relationships;
    - ☐ Loss of employment, business or professional opportunities;
    - ☐ Financial loss;
    - ☐ Negative impact on a credit record, or;
    - ☐ Damage to, or loss of, property

16. If you are reporting the breach to the OIPC, you must include the following information (note: there are fields in this checklist and in the online form that address each of the factors listed below):

- ☐ The name of the public body;
- ☐ The date on which the privacy breach came to the attention of the public body;
- ☐ A description of the privacy breach including, if known,
  - ☐ the date on which or the period during which the privacy breach occurred;
  - ☐ a description of the nature of the personal information involved in the privacy breach; and
  - ☐ an estimate of the number of affected individuals;
- ☐ Contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- ☐ A description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individuals.

Prevention

17. Describe the steps taken to contain and reduce the harm of the breach (e.g. locks changed, computer access codes changed or revoked, computer systems shut down):

18. Describe the long-term strategies you will take to correct the situation (e.g. staff training, policy development, privacy and security audit, contractor supervision strategies, improved technical security architecture, improved physical security):

If you have completed a security audit and are reporting this breach to the OIPC, please forward a copy of the audit with your report.