Fraser Valley Regional District

Issued	
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