

| | |
|---------|--------------|
| Issued | May 27, 2021 |
| Amended | |

PRIVACY AND ACCOUNTABILITY POLICY

PURPOSE AND INTENT

The *Fraser Valley Regional District Privacy and Accountability Policy* sets out the general expectations and legal obligations of the organization with respect to the protection of privacy and Personal Information 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.

This Policy is the foundation of the FVRD’s Privacy Management Program and is intended to demonstrate the FVRD’s commitment and accountability with respect to the protection of privacy and Personal Information in all FVRD programs, activities and operations.

The FVRD commits to taking reasonable security precautions to protect privacy and Personal Information in the course of conducting its business.

FRAMEWORK

The two-fold purpose of FOIPPA provides a process for the public to access records and sets out how privacy and Personal Information is to be protected.

Access to Information

FOIPPA establishes a process by which an individual may request access to information contained in records in the custody or under the control of the FVRD. The right to access information, including Personal Information, is subject to prescribed exemptions from disclosure under FOIPPA. The FOIPPA Head must establish categories of records that are in the custody or under the control of the public body which are available to the public without a request for access to information under FOIPPA.

Protection of Privacy

The protection of privacy provisions of FOIPPA prohibit the unauthorized collection, use and disclosure of Personal Information, while also providing an individual the right to correct their Personal Information which is held by the FVRD.

DEFINITIONS

“Contact Information” means information that would enable an individual to be contacted at a place of business, and includes: name, position or title, business telephone number, email address and fax number, as well as business address.

“FOIPPA Head” means the person designated by the FVRD Board in accordance with FOIPPA as a statutory decision maker for the purpose of administering and complying with FOIPPA in the organization. The FOIPPA Head is typically also designated as the FVRD Privacy Officer who has administrative oversight of the FVRD Privacy Management Program.

“Information Sharing Agreements” (ISAs) means a process when there is regular and systematic exchange of Personal Information between Public Bodies or between Public Bodies and external agencies. ISAs set out the terms and conditions of the exchange of Personal Information in compliance with the provisions of FOIPPA, and any other applicable legislation.

“Office of the Information and Privacy Commissioner” (“OIPC”) 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 Impact Assessment” is an assessment conducted by a public body to determine if a current or proposed enactment, system, project, program, activity or initiative meets the protection of privacy provisions under FOIPPA.

“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.

“Record” means books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

“Service Provider” means a person retained under a contract to perform services for a Public Body.

“Use consistent” means that the use of personal information is consistent with the purpose for which the personal information was obtained or compiled where the use of an individual’s personal information has a reasonable and direct connection to that 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 an individual’s personal information.

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 policy applies to all FVRD employees, Board Members, agents, volunteers, and service providers.

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

- Complying with the protection of privacy provisions of FOIPPA and this policy;
- Consulting with the designated FOIPPA Head regarding the requirements of FOIPPA and this policy;
- Reporting privacy breaches immediately to the designated FOIPPA Head; and
- Participating in privacy training, as required.

The designated FOIPPA Head also assumes the role of the FVRD Privacy Officer and is responsible for the administration of the FVRD Privacy Management Program and for ensuring the FVRD's compliance with its statutory responsibilities under FOIPPA and associated FVRD policies.

POLICY AND PROCEDURE: COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION

The FVRD may only collect, use and disclose Personal Information as expressly authorized under FOIPPA.

Personal Information must be collected directly from the individual the information is about in the absence of consent allowing for the collection of Personal Information from a third party.

Where Personal Information is collected for a prescribed purpose, the individual the Personal Information is about must provide consent in the prescribed manner, as set out elsewhere in this policy.

The FVRD must ensure that an individual from whom it collects Personal Information is told:

- the purpose for which the personal information is being collected;
- the legal authority for collecting it; and
- the title, business address and business phone number of the person designated by the FVRD to answer questions with respect to the collection of the individual’s personal information, in this case, the FOIPPA Head or Privacy Officer.

The FVRD may only collect personal information if it is directly related to a program or activity of the FVRD.

The FVRD must not collect personal information for one purpose and use or disclose it for another purpose.

The FVRD must not “over-collect” personal information and must only collect that amount of Personal Information necessary for purposes of discharging its statutory obligations or for a use consistent with the operation of its programs or activities.

Subject to specified use and disclosure provisions under FOIPPA, the FVRD may generally only use and disclose Personal Information in its custody or under its control for the purpose for which the Personal Information was collected, or for a use consistent with that purpose; or if the individual the information is about has consented to the use and/or disclosure of their personal information in the manner prescribed under FOIPPA.

Where an individual’s consent is required for purposes of collecting, using and disclosing their Personal Information, consent must:

- be in writing;
- done in a manner that specifies the Personal Information for which the individual is providing consent; and
- the date on which the consent is effective and, if applicable, the date on which the consent expires.

The collection of Personal Information through the use of audio taping or video surveillance is strictly prohibited unless authorized by the FOIPPA Head.

The FVRD must make every reasonable effort to ensure that the Personal Information it collects from an individual is accurate with the understanding that an individual has a right under FOIPPA to request the FOIPPA Head to correct the personal information where the individual believes there is an error or omission in their personal information.

Personal Information used to make a decision about an individual must be retained for at least one year. Personal Information will be destroyed in accordance with the FVRD *Records Classification and Retention Policy*.

The FVRD will make reasonable security arrangements to protect Personal Information. Security measures will be appropriate and proportional to the sensitivity of the Personal Information. This includes records containing Personal Information that may be located outside of FVRD offices but which is still within the custody or under the control of the FVRD, including but not limited to personal information contained on mobile devices and/or computers.

The FVRD is committed to the ongoing FOIPPA training of its employees, Board Members, agents, volunteers, and service providers as part of its Privacy Management Program.

A PIA will be completed *prior* to the implementation of any new program or initiative which may include the collection, use or disclosure of Personal Information. The PIA will be overseen by the FOIPPA Head and will include all employees involved in the implementation of the new program or initiative, and information technology employees, and any other employees as deemed

necessary. PIAs may also be conducted with respect to a current program, initiative or activity, in order to determine if the privacy provisions under FOIPPA are being met.

Where the external use and disclosure of FVRD-held Personal Information is required for the operation of a FVRD program, an ISA will be put in place which will establish sufficient parameters and security measures for purposes of protecting privacy and personal information. The ISA will be developed in consultation with relevant employees, the FOIPPA Head, information technology employees and any other employees as deemed necessary.

Personal information in the FVRD's custody or under its control must be stored and accessed within Canada, except in limited circumstances authorized under FOIPPA, and in the absence of an individual's consent as prescribed under FOIPPA.

The FVRD requires all FVRD third party Service Providers, whose work on behalf of the FVRD involves the collection, use, disclosure, storage, retention and/or destruction of Personal Information, to abide by FOIPPA, this policy, and any related contractual requirements. All FVRD third party Service Provider contracts will contain language outlining this requirement.

The FVRD's corporate email will be used solely for the purposes of conducting FVRD business as set out in *the FVRD Assignment of Corporate Email Address Policy and Procedure*.

BREACH OF POLICY

Complaints and suspected breaches of this policy must be reported immediately to the Privacy Officer. The Privacy Officer, or their delegate, may carry out an investigation and is authorized to collect, use and disclose Personal Information contained in the complaint as necessary for the purpose of conducting the investigation, except that the name of the complainant will be held in strict confidence and will not be disclosed.

| | |
|--------------|----------------------|
| Approved by | Board: May 27, 2021 |
| Policy Owner | Legislative Services |