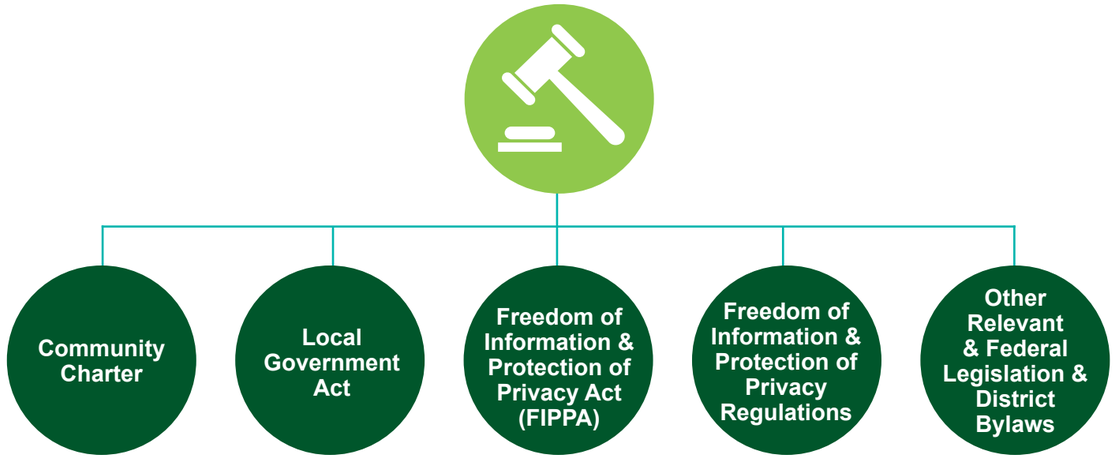
## Legislation




### Privacy Management Program Components

Ensuring consistent application of legislation, including through policies, procedures, standards and reporting.

1. Personal Information Inventories, Directories or Databases
2. Privacy Management Policies
3. Risk Assessment Tools (Privacy Impact Assessment, Security Risk Assessment)
4. Employee Training
5. Breach Response Protocols
6. Compliance Reporting
7. Service Provider Management
8. Communicating with Individuals and Demonstrating Accountability

### Definitions

- **When we use the term “personal information” we mean it according to the definition in FIPPA: recorded information about an identifiable person other than “contact information”**
- **“Contact information” means to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual**

For information or copies of this document, please contact the Saanich Information and Privacy Team:
(250) 475-1775 e-mail: foi@saanich.ca

District of Saanich

# Protecting Personal Information

## Privacy Management Framework

## Core Beliefs

### Personal Information is collected, used & disclosed in the context of our business

The District of Saanich is a public body whose business is done on behalf of and in the best interests of its citizens. The business of the District encompasses all departments and personal information is considered in the context of our records management program. The District has a legal and moral obligation to responsibly manage personal information.

The District of Saanich protects the personal information it collects, uses, and discloses in accordance with the Freedom of Information and Protection of Privacy Act (FIPPA) by:

- promoting a culture of privacy awareness,
- application of sound information access and privacy principles, and
- appropriate and reasonable security measures.

### Objectives of the Privacy Management Program

- Building a corporate culture of privacy awareness
- Collaborating on privacy management across all departments led by a committed Senior Management Team
- Implementing a comprehensive Privacy Management Program in compliance with the privacy legislation and regulations

### Success will mean that:

- Privacy considerations are ‘built by design’ into all District initiatives, programs, and services
- Personal information is responsibly collected, used, and disclosed
- Employees have a sound understanding of responsible privacy practices for their own and the personal information of others

# Privacy Principles

## Accountability

Principle

**Responsibility for personal information protection is accepted at all levels. A Privacy Officer is designated, who provides advice and support related to personal information management.**

Practices

- We provide training and skill development opportunities related to privacy management for all staff.
- If we use personal information to make a decision directly affecting an individual, the information is retained for at least one year after use in accordance with FIPPA and the Records Classification and Retention Schedule (RCRS).

## Openness and Transparency

Principle

**The public has trust and confidence in the District's information access and privacy practices.**

Practices

- We make information available to the public about policies, practices, and compliance measures relating to personal information management.
- We inform the public, employees, and service providers why their personal information is being collected, what it will be used for, and to whom it will be disclosed.
- We tell people how they can access and amend their personal information.

## Consent

Principle

**The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except in certain limited circumstances.**

Practices

- We collect personal information directly from or as authorized by the person concerned.
- We only use personal information for the purpose we collected it for, unless the person consents to us using it for an unrelated purpose.

## Limiting Collection

Principle

**The collection of personal information relates directly to, and is necessary for a program or activity.**

Practices

- We collect personal information for a lawful purpose that is directly related to our functions and activities.
- We maintain a Personal Information Inventory to record the nature of personal information we collect, store, and share.
- We regularly review the nature (amount, sensitivity, elements) of personal information collected.

## Limiting Use, Disclosure, and Retention

Principle

**Personal information is used or disclosed for purposes for which it was collected, except with the consent of the individual or as required by law.**

Practices

- To apply a consistent and comprehensive approach to managing personal information we use the RCRS.
- We implement Information Sharing Agreements to document the purposes and conditions of information access and use between us and other organizations.

## Accuracy

Principle

**Personal information shall be reasonably accurate, complete, and up-to-date.**

Practices

- We make sure that personal information is relevant and accurate before using it.
- We allow people to update, correct or amend their personal information where necessary.

## Security

Principle

**Personal information is protected by security safeguards appropriate to the sensitivity of the information.**

Practices

- We have policies in place to govern the use of technology resources.
- We store and protect records responsibly based on sensitivity of the information and keep personal information no longer than necessary and destroy it appropriately.
- We review service provider contracts and include the privacy protection clauses that address the prohibition of the disclosure of personal information outside Canada except in limited circumstances.

## Individual Access

Principle

**Upon request, an individual shall be informed of the existence, use, and disclosure of personal information and shall be given access to that information.**

Practices

- We tell people how they can access and amend their personal information.
- We tell people who they can contact for access to their information.
- We maintain and make available a directory that lists personal information banks.