SUBJECT: PRIVACY MANAGEMENT	
DATE OF ISSUE: March 6, 2017 May 8, 2017	**ORIGIN:** LEGISLATIVE SERVICES **REFERENCES:** • *Freedom of Information and Protection of Privacy Act* (FIPPA), • Freedom of Information and Protection of Privacy Bylaw No. 9369 • Freedom of Information and Protection of Privacy Policy (1/FOI) • Records Management Policy 1/RECS

PURPOSE

The Privacy Management Policy ("the policy") is the District of Saanich's ("the District"), corporate approach to privacy management. The policy provides a framework for how the District will operate in order to ensure personal information is responsibly managed in accordance with Part 3, Protection of Privacy, of the *Freedom of Information and Protection of Privacy Act.*

The policy strengthens the District's ability to protect the privacy of individuals' personal information by clearly articulating roles and responsibility for privacy management within the District. It identifies the mandatory assessment tools and agreements that must be completed by the District, as well as reporting and audit requirements. Key components of the District's privacy management program include:

- accountability for privacy management requirements;
- development, completion and review of corporate privacy policies that ensure lawful collection, use, disclosure, storage and disposal of personal information;
- development, completion and review of privacy impact assessments;
- development, completion and review of information sharing agreements, and other agreements as outlined in FIPPA;
- management of the personal information inventory;
- management of privacy breach incidents and complaints;
- development, completion, review and implementation of compliance and auditing tools and processes; and
- on-going employee privacy awareness and education.

SCOPE

The policy applies to all District of Saanich employees and elected officials.

DEFINITIONS

The following definitions are provided for key terms and acronyms used in this document.

"Common or Integrated Program or Activity" means a program or activity that provides one or more services through (i) one or more other public bodies or agencies working collaboratively, or (ii) one public body working on behalf of one or more other public bodies or agencies, (iii) is confirmed by regulations under FIPPA as being a common or integrated program or activity; and (iv) is confirmed by a written agreement that complies with regulations under FIPPA.

"**Contact Information**" means information to enable an individual at a place of business to be contacted, including the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

"Employee" includes a person who is employed by the District, a member of Council, a volunteer, and a service provider.

"FIPPA" means the *Freedom of Information and Protection of Privacy Act* (British Columbia) as it is in force from time to time.

"FIPPA Clerk" means a person(s) designated by the District to coordinate on behalf of a District Department, access to records requests under FIPPA, and to administer Department personal information holdings, all in co-ordination with, as applicable in the circumstances, the Privacy Officer, the Information and Privacy Advisor or the Head.

"Foreign Demand for Disclosure" means a subpoena, warrant, order, demand or request that is (i) from a foreign state or another authority outside of Canada, and (ii) for the unauthorized disclosure of personal information to which FIPPA applies.

"Head" means a person designated by the District as the District's head for the purposes of FIPPA.

"Information and Privacy Advisor", means the person designated by the District to prepare responses to requests for access to records under FIPPA and to provide related advice to employees and the public.

"Information Sharing Agreement" or **"ISA"** means an agreement between the District and another public body under FIPPA; a government institution subject to the *Privacy Act* (Canada); an organization subject to the *Personal Information Protection Act* (British Columbia) or the *Personal Information Protection and Electronics Documents Act* (Canada); a public body, government institution or institution as defined in applicable provincial legislation have the same effect as FIPPA; a person or group of persons; or an entity prescribed in the FIPPA regulation, which agreement sets conditions on the collection, use or disclosure of personal information by the parties to the agreement.

"Personal Information" means recorded information about an identifiable individual other than contact information.

"Personal Information Bank" or "**PIB"** means a collection of personal information that is organized or retrievable by the name of an individual or by identifying number, symbol or other particular assigned to an individual.

"Personal Information Inventory" or "**PII"** means a directory listing and describing personal information holdings held by the District.

"Policy" means the privacy management policy of the District.

"Privacy Breach" means access to, or collection, use, disclosure or disposal of personal information, whether accidental or deliberate, that is not authorized under FIPPA.

"Privacy Impact Assessment" or "**PIA"** means a process that is conducted by the District to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of FIPPA.

"Privacy Officer" means the position designated by the District to be responsible for managing the District's privacy management program, implementation of the policy within the District, and compliance with FIPPA.

"Privacy Protection Schedule" means a schedule of contract terms that forms part of a contract between the District and a service provider that involves personal information and requires the service provider comply with its statutory obligations under FIPPA with respect to personal information and other privacy-related obligations of the service provider as set out in the schedule.

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

"Service Provider" means a person retained under contract to perform services for the District.

1. POLICY STATEMENT

1.1 The policy is established in accordance with the District's *Freedom of Information and Protection of Privacy Act Bylaw No. 9369*.

1.2 The District protects the personal information it collects, uses, and discloses in accordance with FIPPA, by promoting privacy awareness, application of sound privacy principles, and implementation of reasonable security measures to protect personal information.

1.3 The policy is the foundation for the District's privacy management program. It sets the framework for privacy to be a central component of the District's business practices and a built-in component of day-to-day program operations.

2. AUTHORITIES

2.1 A position designated as Head, has the authority and responsibility to manage and implement the policy.

3. ROLES & RESPONSIBILITIES

3.1 Chief Administrative Officer

- Approves policy and procedures and ensures all employees are given notice of, and access to a copy of the policy.

3.2 Department Heads

- Lead the District in creating and maintaining an enhanced awareness of privacy protection and in the responsible collection, use, disclosure, storage and disposal of personal information.
- Meet regularly with, and support the Privacy Officer in carrying out his or her duties and responsibilities, including under the policy.
- Assign resources to support compliance with the policy and FIPPA.
- Co-operate with the Privacy Officer and a Head in implementing the policy and in complying with FIPPA.
- Implement all actions required by the privacy impact assessment.
- Implement all actions required by the information sharing agreement.

3.3 Privacy Officer

- Coordinates and manages the policy's implementation and any corporate directions, policies, guidelines and templates that flow from the policy.
- Manages and coordinates the privacy management program, including monitoring and reviewing its implementation, and recommending necessary resources, actions and revisions to the policy and to the District's FIPPA compliance administration and resources more generally.
- Liaises with the Office of the Information and Privacy Commissioner, or OIPC, including in relation to investigations.
- Reviews and comments on all privacy impact assessments, information sharing agreements and other privacy-related agreements.
- Maintains a personal information inventory.
- Coordinates employee training and education and ensures that all new employees receive FIPPA orientation during initial on-boarding with the District and training within the first year of their employment, including regarding the collection, use, disclosure, storage and disposal of personal information, as appropriate to their work function.
- Conducts compliance reviews and audits in order to assess compliance with FIPPA and the policy and communicates results regularly to the District's Chief Administrative Officer and Department Heads.

3.4 FIPPA Clerk

- Ensures that records are accessible to those who need them and are authorized to use them.
- Remains current and knowledgeable about the types of records made routinely available within the department, and remains aware of circumstances that may require an applicant to file a formal request under FIPPA.
- Remains current and knowledgeable of and administers Department personal information holdings.

- Participates in the privacy management program (attends meetings of the working group, advocates protection of personal information within the department).

3.5 Employees

- Comply with the policy and other privacy-related policies, guidelines, templates and directions of the District.
- Complete training on FIPPA, including regarding the collection, use, disclosure, storage and disposal of personal information, as appropriate to their work function.
- Conduct privacy impact assessment and information sharing agreements in the manner and form directed by the Privacy Officer, and to keep the Privacy Officer informed of changes to initiatives that require updates to the privacy impact assessment or information sharing agreement.
- Support the Privacy Officer in ensuring the personal information bank and personal information inventory are accurate and complete, as appropriate to their work function.
- Immediately report actual or reasonably suspected privacy breaches as set out in the policy.
- Report privacy complaints to the Privacy Officer.
- Include the privacy protection schedule or privacy protection language, as deemed appropriate by the Privacy Officer, in all contracts with service providers that involve collection, use or disclosure of personal information.
- Inform the Privacy Officer or Information and Privacy Advisor of requests for access to or correction of personal information.
- Co-operate with the Privacy Officer and a Head in implementing the policy and in complying with FIPPA.

4. EDUCATION AND AWARENESS

4.1 Privacy training for employees, as appropriate to their work functions, is required as set out below:

4.1.1 For all employees: training on FIPPA and privacy generally as appropriate to their work function.

4.1.2 For employees handling high-risk or sensitive personal information electronically, in co-ordination with the IT department's training, training related to information systems and their security.

4.1.3 For employees managing programs or activities, training related to privacy impact assessments.

4.1.4 For employees managing common or integrated programs or activities, training related to information sharing agreements.

5. PRIVACY IMPACT ASSESSMENT or PIA

5.1 Privacy impact assessments are to be conducted by Department or program area employees in accordance with the District's PIA template.

5.2 Department Heads shall ensure privacy impact assessments are submitted to the Privacy Officer for review and comment, at the earliest practicable opportunity during the development of any proposed enactment, system, project, program or activity - from now on referred to generally as an "initiative, and should be signed off before the initiative starts. A PIA must also be submitted during the development of any proposed updates to a current initiative.

5.3 Department Heads or designated program area employees are to prepare and complete the privacy impact assessment. The Privacy Officer will review it in order to ensure that the privacy impact assessment is completed appropriately. The privacy impact assessment is to be signed by the appropriate District authorities, including the Privacy Officer, acknowledging and confirming content.

5.4 The Privacy Officer will ensure that the original of each approved privacy impact assessment is retained in the Legislative Services Department.

5.5 Department Heads will implement all actions required by the privacy impact assessment.

5.6 The Privacy Officer will develop, maintain and review the District's internal processes to ensure completion of appropriate privacy impact assessments within the District, in accordance with the policy.

6. INFORMATION SHARING AGREEMENT or ISA

6.1 Information sharing agreements are to be completed by Department Heads or designated program area employees using the District's information sharing agreement template. An information sharing agreement is completed once it has been fully signed by all required parties.

6.2 The Privacy Officer will ensure completion of, and conduct reviews of, all information sharing agreements and ensure they are updated when changes have been made to the initiative.

6.3 Department Heads will ensure implementation of all actions required by the information sharing agreement.

7. PERSONAL INFORMATION INVENTORY or PII and BANK or PIB

7.1 The District will maintain a personal information inventory documenting details of the personal information holdings of the District and will involve collaboration with all Departments.

7.2 The Privacy Officer, in collaboration with the Records Coordinator, will document personal information banks and information sharing agreements that result from new enactments, systems, projects, programs, or activities of the District in the personal information inventory.

8. PRIVACY BREACH MANAGEMENT

8.1 The Privacy Officer, in consultation with a Head, is responsible for the coordination, investigation, and risk management of privacy breaches.

8.2 There are four key steps in responding to a privacy breach. The steps may occur concurrently, in quick succession, or in a different order. The first three steps must be undertaken as soon as possible following the breach. The fourth step involves investigation into the cause of the breach and may require a security audit of both physical and technical security.

Step 1 **Containment** of the breach, **recovery** of confidential or personal data and **reporting** the incident;

Step 2 **Investigation** and **evaluation** of the risks of the unauthorized disclosure of personal information;

Step 3 **Notification** of individual(s) affected as determined necessary;

Step 4 **Prevention** strategies to safeguard against future breach incidents.

9. ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

9.1 Employees receiving a formal request under FIPPA for access to or correction of an individual's personal information in the custody or control of the District are to forward the request to the Information and Privacy Advisor promptly for response.

9.2 Employees receiving a routine request from an individual to correct their factual personal information, such as a change of or update to a residential or mailing address, e-mail address or phone number, can make the requested change.

10. PRIVACY RELATED COMPLAINTS

10.1 Employees receiving a complaint related to the District's collection, use or disclosure of personal information are to refer the complainant to the Privacy Officer or the Information and Privacy Advisor promptly for response.

11. ACCURACY OF PERSONAL INFORMATION

11.1 The District will make every reasonable effort to ensure that the personal information it relies on to make a decision directly affecting an individual is accurate and complete.

11.2 The District will document and keep current the processes it uses, or that are used on behalf of the District, to use personal information in making a decision directly affecting an individual.

12. FOREIGN DEMANDS FOR DISCLOSURE

12.1 An employee who receives or is aware of a foreign demand for disclosure is to immediately notify the Privacy Officer.

13. SERVICE PROVIDER MANAGEMENT

13.1 Employees who prepare or manage contracts are to include the privacy protection schedule or standard privacy language, as designated by the Privacy Officer, in all contracts that involve the service provider having access to, or collecting, using or disclosing, personal information in the custody or under the control of the District.

14. COMPLIANCE REVIEWS AND AUDITS

14.1 The Privacy Officer will, on a regular basis, conduct compliance reviews and audits in order to assess compliance with FIPPA and the policy and will communicate results to the Corporate Administrative Officer and the Department Heads.

15. PROTECTION OF PERSONAL INFORMATION

15.1 The District will 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.