DISTRICT OF
OAK BAY

Policy	Privacy Management
Approved By:	CAO
Approval Date:	December 7, 2020
Amendment Date:	

PURPOSE

The Privacy Management Policy ("the Policy") is the District of Oak Bay's corporate approach to privacy management. The Policy provides a framework for how the District will operate 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*. ("*FOIPPA*")

This Policy strengthens the municipality's ability to protect the privacy of individuals' personal information by clearly articulating roles and responsibility for privacy management within the District.

SCOPE

The Policy applies to all District of Oak Bay employees, elected officials and volunteers, who shall comply with all duties and obligations set out in *FOIPPA*. This Policy is intended to ensure compliance with *FOIPPA*. To the extent that any portion of this Policy conflicts, or can be interpreted to conflict, with any provision of *FOIPPA*, the provision of *FOIPPA* will apply.

DEFINITIONS

Personal Information: information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to identify directly or indirectly an individual. Individuals, for this purpose, include prospective, current, and former customers, employees, and others with whom the District has a relationship. Most information collected by the District about an individual is likely to be considered personal information if it can be attributed to an identified individual.

Some examples of Personal Information are as follows:

- the individual's name, address, or telephone number;
- the individual's race, national or ethnic origin, colour, or religious or political beliefs or association;
- the individual's age, sex, sexual orientation, marital status, or family status;
- an identifying number, symbol, or other identifier assigned to the individual;
- the individual's fingerprints, blood type or inheritable characteristics;
- the individual's consumer purchase history

Privacy: the right and obligations of individuals to control the flow of their Personal Information, including the collection, use and disclosure of that information. This is known as the right of informational self-determination.

RESPONSIBILITIES

Privacy Program Management

The Corporate Officer has overall responsibility for developing and managing the privacy program for the District of Oak Bay, is designated as the Head for the purposes of *FOIPPA*, and has mandatory duties under *FOIPPA* and District of Oak Bay *Records Administration Bylaw No. 3827, 1994*.

As Head, the Corporate Officer, or his/her designate, is responsible for:

- Providing advice and training related to protection of privacy and record-keeping.
- Monitoring compliance with privacy legislation.
- Mitigating risk to the organization and ensures compliance by conducting privacy impact assessments.
- Investigating and resolving privacy complaints and breaches.
- Representing the District of Oak Bay during Information and Privacy Commissioner investigations and audits.
- Overseeing the corporate records management system, documenting procedures and best-practices for managing records, managing routinely releasable information and forms creation.
- Providing advice to departments, escalating privacy issues, and processing Freedom of Information requests.
- Liaising with the Office of the Information and Privacy Commissioner, or OIPC, including in relation to investigations.
- Reviewing and commenting on all privacy impact assessments, information sharing agreements and other privacy-related agreements.
- Conducting reviews in order to assess compliance with this Policy, FOIPPA and ,communicating the results to the District's Chief Administrative Officer and Directors.
- Recommending necessary resources, actions and revisions to this Policy and to the District's FOIPPA compliance administration and resources more generally.

Information Technology (IT) is responsible for:

- Assisting with investigation and risk assessment of privacy breaches and, in the event of theft or criminal activity, communicating to police.
- Completing IT Security Risk Assessments in collaboration with all privacy impact assessments that involve IT systems including cloud computing.

Employee, Elected Official and Volunteer Responsibilities

Privacy is the responsibility of every employee, elected official and volunteer. As employees, elected officials and Volunteers of the District of Oak Bay covered by *FOIPPA*, each individual is responsible for:

- Handling personal information in accordance with *FOIPPA* and safeguarding the personal information that is handled to ensure the privacy of individuals who interact with the District of Oak Bay.
- Recognizing that that *FOIPPA* requires the District to make every reasonable effort to respond openly, accurately, completely and without delay, and that requests for responsive records are time sensitive.
- Immediately reporting actual or reasonably suspected privacy breaches, as well as any privacy complaints to the Corporate Officer.
- Ensuring that privacy protection language, as deemed appropriate by the Corporate Officer, is included in all municipal forms and contracts with service providers that involve collection, use or disclosure of personal information.
- Informing the Corporate Officer of requests for access to or correction of personal information.
- Cooperating with the Corporate Officer in implementing the Policy, complying with FOIPPA and managing any privacy breaches.

Directors, Managers and Supervisors are additionally responsible for:

- Exercising due diligence and implementing privacy requirements in their area of responsibility.
- Ensuring that employees understand and comply with privacy legislation and policies. Human Resources will also communicate relevant policies through new employee orientation sessions.
- Completing Privacy Impact Assessments (PIA) for department programs, projects and business processes.
- Implementing all actions required by this Policy or by the Corporate Officer in relation to this Policy or FOIPPA.
- Assigning resources to support compliance with this Policy and FOIPPA as required.

EDUCATION AND TRAINING

Training is provided on an annual basis and attendance at privacy awareness training is mandatory for all employees. The training program is reviewed and updated annually to reflect current legislative, regulatory, industry, and District Policy and procedures requirements.

PRIVACY IMPACT ASSESSMENTS (PIA)

Corporate Services assesses potential privacy impacts when new processes involving Personal Information are implemented, and when changes are made to such processes including any such activities outsourced to third parties or contractors.

The purpose of PIAs is to ensure that the District of Oak Bay programs, business processes and systems fulfil legislated obligations and Policy requirements. While completing a PIA, the actual or potential effect on privacy is assessed and ways to mitigate adverse impacts are identified.

- The business area that is responsible for, or sponsors, the program, project, or business process completes the PIA with the assistance of the Corporate Officer or designate.
- The Information Technology section contributes to PIAs on District of Oak Bay systems.
- Privacy Impact Assessments are signed by the appropriate Director or Manager, the Corporate Officer, and the Information Technology support person.

INFORMATION SHARING AGREEMENTS

Where Personal Information is provided to parties outside the District on a regular and systematic basis, the terms of disclosure are documented in a formal information sharing agreement. The agreement establishes relationships, responsibilities, security and compliance requirements, access rights and authentication requirements between the parties. Information sharing agreements are reviewed and updated regularly.

PRIVACY BREACHES

The Corporate Officer is responsible for the coordination, investigation, and risk management of privacy breaches. Employees may be asked by the Corporate Officer to assist with the investigation, as appropriate.

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.

NOTICE OF COLLECTION, PURPOSE, AND CONSENT

Personal Information collected by or for the District must only be collected for an identified municipal program or activity.

Unless indirect collection is authorized under FOIPPA, an individual from whom Personal Information is collected must be informed of the following:

- The purpose for collection of Personal Information;
- The legal authority for collecting Personal Information; and
- The title and business contact information of an employee who can answer an individual's questions about the collection of Personal Information.

Where necessary, informed consent for collection and use of Personal Information will be obtained prior to its collection.

USE, RETENTION AND DISPOSAL

The District limits the use of Personal Information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The District retains Personal Information for only as long as necessary to fulfill the stated purposes or as required by law or regulations, and thereafter appropriately disposes of such information in accordance with the *Corporate Records Management Bylaw, 2020.*

Personal Information is stored, managed and accessed solely within Canada, except in limited circumstances specified under *FOIPPA*. The information is anonymized or destroyed promptly and securely as soon as it is no longer needed for the purpose(s) for which it was collected and for legal or business purposes.

ACCESS

Individuals are given informal access to information about themselves, unless *FOIPPA* exceptions apply to the disclosure. Where access is not provided, the individual is informed of the reasons and referred to the Office of the Information Privacy Commissioner if they wish to make a formal request for review.

Individuals may also ask for an explanation of how their Personal Information was used or disclosed, as well as correction of errors or omissions in their Personal Information.

DISCLOSURE

The District discloses Personal Information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

Disclosure of Personal Information without the individual's consent is limited to the circumstances specified under *FOIPPA*. Where *FOIPPA* permits disclosure of the information, the particulars of the case are analyzed, and judgement or discretion is exercised before deciding or not to release the information. Authority for the disclosure is verified prior to the release and the disclosure is documented in writing.

Where consent is required, the person the information is about is clearly informed of the proposed disclosure of their information. Consent is documented in writing.

SECURITY FOR PRIVACY

Personal Information is always protected by physical, technical and organizational security measures that prevent the unauthorized access, collection, use, disclosure, copying, modification and disposal of Personal Information. Security measures are consistent with the sensitivity of the Personal Information and the format in which the information is held.

MONITORING AND ENFORCEMENT

Individuals are informed about how to contact the District with inquiries, complaints and disputes, and a process is in place to address inquiries, complaints, and disputes. Each complaint is addressed, and the resolution is documented and communicated to the individual.

Instances of noncompliance with privacy policies and procedures are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.

SUPERVISORY RECORDS RELATED TO EMPLOYEES

The District's commitment to preserving the confidentiality and privacy of its employees requires that information, such as home phone numbers, addresses or performance evaluations, is used appropriately and not shared, except with authorized personnel and some external parties authorized to obtain the information under *FOIPPA*.

The following apply to supervisory records about employees in their area of responsibility:

- Supervisors ensure that information about their employees is obtained, used, or disclosed according to *FOIPPA* and District policies.
- Only information that is required to manage the employee-employer relationship is obtained and recorded.
- Information is restricted to accurate, objective, factual information that directly relates to managing employee performance or to applying the provisions of the Collective Agreement.
- Each document relates to only one employee and is filed in a working folder dedicated to that employee.
- Employee information is stored only on District premises.
- Documents that contain Personal Information are kept in a secure area and disposed of in accordance with the *Corporate Records Management Bylaw No 4768, 2020.*
- Employee information may be shared with other District staff on a need-to-know basis if they need the information to perform their duties (e.g.: Payroll, Labour Relations, and Occupational Health).

- Requests from outside parties, such as ICBC or Employment Insurance, are referred to Human Resources.
- Access by third parties, including shop stewards, may be granted with the employee's written informed consent providing *FOIPPA* exceptions do not apply.
- Where access is not provided because *FOIPPA* exceptions may apply, the employee or representative is advised that they may make a formal request under the Act.

RELATED BYLAWS AND POLICIES

- Records Administration Bylaw No 3827, 1994
- Corporate Records Management Bylaw No. 4768, 2020
- Records and Information Management Policy
- Electronic Communication for Records Management Policy
- Information Technology Acceptable Use Policy

Lou Varela, Chief Administrative Officer

Dec 8/20

Date