City of Surrey Policy

Department:	Legislative Services	**Policy Title:**	Privacy Policy
Policy Date:	June 8, 2017	**Last Updated:**	Dec 23, 2021
Approved By:	City Clerk		

Policy Statement

This policy outlines a comprehensive privacy framework, elements of which address accountabilities and best practices as related to Fair Information Practices and the Freedom of Information and Protection of Privacy Act (FIPPA).

1. Reason for Policy

The privacy policy guides the City of Surrey in identifying measurable criteria that meet privacy andsecurity objectives and form the basis for the City's privacy program.

2. 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 City has a relationship. Most information collected by the City 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:

- Name
- Home address or personal e-mail address
- Identification number (for example, a Social Security or Social Insurance Number)
- Physical characteristics
- 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.

3. Responsibilities

3.1 Privacy Program Management

The City Clerk has overall responsibility for developing and managing the privacy program forthe City of Surrey, is designated as the Head for the purposes of *FIPPA*, and has mandatory duties under *FIPPA* and City of Surrey, Freedom of Information Bylaw, No. 13662.

Legislative Services 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 impactassessments.
- Investigating and resolving privacy complaints and breaches.
- Representing the City of Surrey during Information and Privacy Commissionerinvestigations and audits.
- Overseeing the Corporate File Plan, documenting procedures and best-practices formanaging records, managing routinely releasable information and forms creation.
- Providing advice to departments, escalates privacy issues, and processes Freedom ofInformation requests.

Information Technology (IT) is responsible for:

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

3.2 Staff

Privacy is the responsibility of every staff member. As employees of the City of Surrey covered by *FIPPA*, staff is responsible for:

- Handling personal information in accordance with *FIPPA* and safeguarding the personal information that is handled in order to

ensure the privacy of individuals who interact withthe City of Surrey.

- Recognizing that *FIPPA* requires the City to make every reasonable effort to respond openly, accurately, completely and without delay, and that requests for responsive recordsare time sensitive.

3.3 Managers/Supervisors

Managers and supervisors are responsible for:

- Exercising due diligence and implementing privacy requirements in their area ofresponsibility.
- Ensuring that staff understand and comply with privacy legislation and policies.
- Completing Privacy Impact Assessments (PIA) for department programs, projects andbusiness processes.

4. Communication

4.1 Human Resources

The City of Surrey Human Resource department communicates relevant policies through themandatory New Employee Orientation sessions.

4.2 Legislative Services

The Records and Privacy Manager communicates the privacy policies and procedures to staffthrough mandatory Privacy Awareness sessions.

4.3 Social Media

The Social Media Policy assists staff in understanding the advantages of social media and therisks associated with confidential information.

4.4 Public

The City of Surrey website contains a privacy policy statement that communicates the City's commitment to privacy to the public, and information regarding the process for individuals torequest City records.

5. Training

Privacy Awareness training is mandatory for all employees. Privacy Awareness courses are reviewed and updated regularly to reflect current legislative, regulatory, industry, and Citypolicy and procedures requirements.

6. Privacy Impact Assessments

Legislative Services assesses potential privacy impacts when new processes involving personal information are implemented, and when changes are made to such processes including any suchactivities outsourced to third parties or contractors.

The purpose of PIAs is to ensure that the City of Surrey programs, business processes and systems fulfil legislated obligations and policy requirements. While completing a PIA, the actualor 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 businessprocess completes the PIA with the assistance of the Records and Privacy Manager.
- The Information Technology Security section contributes to PIAs on City of Surrey systems.
- Privacy Impact Assessments are signed by the Business Owner, Records and PrivacyManager, City Clerk, the Cyber Security Manager (if it involves IT).

7. Information Sharing Agreements

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

8. Privacy Breaches

A formal, privacy breach management process has been implemented, which specifies thefollowing:

- All incidents are reported to the City Clerk who assesses if it is a privacy breach and classifiesthe severity of the incident, initiates required actions, and determines the required involvement by individuals who are responsible for

privacy and security.

- The City has a breach notification procedure supported by clear escalation paths. For additional information, refer to the Privacy Breach Policy.

9. Notice

The City provides notice about its By-laws, privacy policies and procedures and identifies thepurposes for which personal information is collected, used, retained, and disclosed.

10. Choice and Consent

The City provides choices to the individual and obtains implicit or explicit consent with respectto the collection, use, and disclosure of personal information.

11. Collection

The City collects personal information only if such collection is authorized by or under legislation, essential for operating programs or activities, or collected for law enforcementpurposes.

The City has established procedures for review of forms which collect personal information.

12. Use, Retention and Disposal

The City 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 City 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 SurreyCorporate Records By-law, 2010, No. 17002.

The City may disclose personal information outside of Canada only if the disclosure is inaccordance with the regulations.

13. Access

Individuals are given informal access to information about themselves, unless *FIPPA* 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 formalrequest for review.

Individuals may also ask for an explanation of how their personal information was used ordisclosed, as well as correction of errors or omissions in their personal information.

14. Disclosure

The City discloses personal information to third parties only for the purposes identified in thenotice 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 *FIPPA* and to the minimum required (least-privilege). Where *FIPPA* 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. Authorityfor 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 theproposed disclosure of their information. Consent is documented in writing.

15. Security for Privacy

Personal information is protected at all times by physical, technical and organizational security measures that prevent the unauthorized access, collection, use, disclosure, copying, modificationand disposal of personal information. Security measures are consistent with the sensitivity of thepersonal information and the format in which the information is held.

16. Quality

Personal information is accurate and complete for the purposes for which it is to be used.

17. Monitoring and Enforcement

Individuals are informed about how to contact the City 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 reportedand, if needed, corrective and disciplinary measures are taken on a timely basis.

18. Privacy Language in Contracts (Including Service-Level Agreements with Third Parties)

The City's privacy obligations extend to personal information transferred to a contractor forprocessing or information the contractor accesses or collects on the City's behalf.

Contract administrators take appropriate measures to ensure contract terms and

services protectpersonal information.

A Privacy Protection Schedule is included in contracts that involve personal information.

19. Supervisory Records about Employees

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

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

- Supervisors ensure that information about their employees is obtained, used or disclosedaccording to *FIPPA* and City policies.
- Only information that is required to manage the employee-employer relationship isobtained and recorded.
- Information is restricted to accurate, objective and factual information that directly relatesto 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 tothat employee.
- Employee information is stored only on City premises
- Documents that contain personal information are kept in a secure area when they are in use,in a locked area when not in use, and disposed of in accordance with the Surrey Corporate Records By-law, 2010, No. 17002.
- Working folders are reviewed at least once a year to remove outdated and unnecessary documents. All permanent records are sent to Human Resources for filing in the employee'spermanent file.
- Employee information may be shared with other City staff on a need-to-know basis if theyneed 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 toHuman Resources.
- Access by third parties, including shop stewards, may be granted with the employee'swritten informed consent providing *FIPPA* exceptions do not apply.
- Where access is not provided because *FIPPA* exceptions may apply, the employee or representative is advised that they may make a formal request under the *Freedom of Information and Protection of Privacy Act*.