CITY OF VANCOUVER

Corporate Policy

POLICY TITLE	Privacy Policy
CATEGORY	Administrative
POLICY NUMBER	ADMIN-029
POLICY OWNER	Access to Information and Privacy Division City Clerk's Office
ACCESS	Public

PURPOSE

This policy establishes the City of Vancouver's privacy obligations for the collection, use, disclosure, access, storage, retention, and disposal of Personal Information, as required by the *Freedom of Information and Protection of Privacy Act* of British Columbia, (the Act or FIPPA), other legislation and fair information practices.

SCOPE

This policy applies to all City of Vancouver employees, agents, volunteers, service providers, elected officials, and political staff.

This policy does not apply to other Public Bodies differentiated from the City of Vancouver under the Vancouver Charter, Schedule 2 of FIPPA or other governing legislation.

DEFINITIONS

Agent is an entity authorized to act for or in the place of another.

Contact Information is information 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.

Control is the power or authority to manage a Record throughout its life cycle, including restricting, regulating, and administering its use or disclosure.

Custody is having physical possession of a Record in addition to some right to deal with the Record and some responsibility for its care and protection. Custody normally includes responsibility for access, managing, maintaining, preserving, disposing, and providing security of the Record.

Data Security and Privacy Compliance Schedule is a legally binding schedule that is attached to any contract between a public body and a service provider (contractor) that involves the collection, creation, use, disclosure, or storage of personal information controlled by the public body.

Head is the person designated in the City of Vancouver's Freedom of Information and Protection of Privacy By-law as the Head of the Public Body in accordance with section 77 of FIPPA.

Information Sharing Agreement (ISA) is an agreement between a Public Body and at least one other Public Body or entity that sets conditions on the collection, use or disclosure of Personal Information by the parties to the agreement.

Personal Information is recorded information about an identifiable individual other than Contact Information. (see also Sensitive Personal Information)

Personal Information Bank (PIB) is a collection of Personal Information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

Privacy Breach means the theft or loss, or the collection, use or disclosure that is not authorized by FIPPA, of personal information in the Custody or under the Control of a Public Body. (see also Privacy Incident)

Privacy Complaints are concerns raised by members of the public, organizations, City employees or agents in relation to the City's handling of their Personal Information.

Privacy Impact Assessment (PIA) is a mandatory assessment that is conducted by a Public Body to determine if a current or proposed enactment, project, program or activity that involves personal information meets or will meet the privacy requirements of FIPPA.

Privacy Incident includes any event that has or could result in the theft or loss or the unauthorized collection, use, or disclosure of Personal Information. (see also Privacy Breach)

Privacy Response Protocol is a program control document that outlines steps in managing a known or suspected privacy breach.

Public Body includes a) a ministry of the government of British Columbia, b) an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2 of FIPPA, or c) a Local Public Body (as defined in Schedule 1 of FIPPA).

Records are 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, (as defined in Schedule 1 of FIPPA).

Sensitive Personal Information is personal information with a higher risk of harm to individuals if the information is improperly collected, used or disclosed and may impact an individual's personal safety. (see also Personal Information)

POLICY STATEMENTS

1. COMPLIANCE WITH FIPPA

All persons affiliated with the City, including employees, agents, volunteers, service providers, elected officials, and political staff, shall comply with all duties and obligations set out in FIPPA. This policy is intended to ensure compliance with FIPPA. To the extent that any portion of this policy conflicts, or can be interpreted to conflict, with any provision of FIPPA, the provision of FIPPA will apply unless expressly set out herein.

2. ACCOUNTABILITY

2.1. City Manager

The City Manager is delegated as Head for the purposes of the City of Vancouver's statutory responsibilities under FIPPA. The "Head" is authorized to delegate their FIPPA responsibilities to any other City of Vancouver staff position.

2.2. Director, Access to Information & Privacy (ATIP)

The Director, Access to Information & Privacy (ATIP), is legally delegated by the City Manager to fulfill all City of Vancouver FIPPA "Head" responsibilities with the exception of determining what information must be disclosed in the public interest.

The ATIP Director is responsible for:

- Developing, implementing, and maintaining the City's Access to Information and Privacy Program;
- Investigating and responding to Privacy Complaints and Privacy Incidents as per the privacy protocol;
- Assisting employees with the completion of PIAs and ISAs;
- Providing privacy training to employees;
- Providing advisory services to employees;
- Maintaining the City of Vancouver's PIB;
- Recommending remedial action in response to a breach of this policy or FIPPA;
- Representing the City before the Office of the Information and Privacy Commissioner (OIPC); and
- Delegating duties assigned under this Privacy Policy.

2.3. Management

Management is responsible for:

- Complying with the privacy protection requirements in FIPPA and this policy;
- Communicating the requirements of FIPPA and this policy to employees in their business units;

- Ensuring that Personal Information in the Custody and Control of their business unit is handled in accordance with FIPPA and this policy;
- Conducting and completing PIAs prior to implementing new initiatives or significantly changing existing initiatives that involve Personal Information; and
- Establishing ISAs, when required.

2.4. Employees/Volunteers/Agents

All employees, agents, volunteers, elected officials, and political staff, are responsible for:

- Complying with the privacy protection requirements in FIPPA and this policy;
- Consulting with their volunteer coordinator or manager and/or ATIP regarding the requirements in FIPPA and this policy;
- Reporting Privacy Incidents to their supervisors and ATIP;
- Following instructions outlined by the ATIP Director and/or delegate; and
- Participating in privacy training, as required.

2.5. Service Providers

The City requires all third party service providers, whose work on behalf of the City involves the collection, use, access, disclosure, storage, retention or destruction of Personal Information, to abide by this policy, the contractual Data Security and Privacy Compliance Schedule, and FIPPA.

3. COLLECTION

The City must have legal authority to collect Personal Information. Collection must only occur as permitted under FIPPA.

Only the minimum amount of Personal Information will be collected to perform required City functions.

Unless otherwise permitted by FIPPA, Personal Information will only be collected directly from the individual who the Personal Information is about.

4. NOTICE OF COLLECTION, PURPOSE, AND CONSENT

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

Unless indirect collection is authorized under FIPPA, 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 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.

5. USE, DISCLOSURE, AND ACCESS

Personal Information shall only be used, disclosed, or accessed:

- For the purpose for which it was collected;
- For a use that is consistent with the purpose for which it was collected;
- With the consent of the individual the information is about; or
- When a specific use, access, or disclosure is authorized by legislation.

Personal Information is only to be used, disclosed or accessed as is required for the purposes of fulfilling work-related duties at the City.

For regular, systematic sharing of Personal Information, ISAs may be required to establish sufficient parameters and security measures around external use and disclosure of City-held Personal Information.

6. ACCESS, ACCURACY, AND CORRECTION OF PERSONAL INFORMATION

If Personal Information is used by or on behalf of the City to make a decision about an individual, the City must make every reasonable effort to ensure that the Personal Information is accurate and complete.

Except in limited circumstances, individuals have the right to access their own Personal Information upon request.

Individuals have the right to request correction of their factual Personal Information. A notation must be placed in the documentation if a correction cannot be applied. The individual must be advised of the reason their request was not applied.

7. STORAGE AND ACCESS INSIDE AND OUTSIDE OF CANADA

The City must make every reasonable effort to ensure personal information in the Custody and Control of the city is stored and/or accessed in Canada.

If personal information in the custody or control of the city is to be stored and/or accessed outside of Canada a PIA must be completed and include a supplemental assessment and approved by the Head.

8. SECURITY AND PROTECTION

The City will employ reasonable safeguards to prevent the unauthorized collection, use, access, disclosure, storage, or disposal of Personal Information. Security arrangements will include appropriate technological, physical, and administrative safeguards.

9. RETENTION AND DISPOSITION

The City will retain an individual's Personal Information for at least one year when it is used to make a decision that directly affects an individual.

The City will retain and dispose of Personal Information in accordance with the City's Records Management By-Law and Corporate Records and Information Management Policy.

10. OPENNESS

This policy, associated procedures, and the City's information-handling practices will be made readily available to the public.

11. BREACHES OF FIPPA AND PRIVACY OFFENCES

If Personal Information or Sensitive Personal Information in the Custody or Control of the City is collected, used, or disclosed in a manner that is not authorized by FIPPA, a Privacy Breach will occur. A Privacy Breach under FIPPA will also constitute a breach of this Policy.

All Privacy Incidents must be reported to the ATIP Director immediately upon discovery. In accordance with the Privacy Response Protocol, the ATIP Director and/or their delegate will lead an investigation to confirm if a Privacy Breach has occurred.

If a confirmed Privacy Breach poses a risk of significant harm to individuals, the City is required to provide notifications to the affected individuals and the OIPC. Notifications to affected individuals will not be required if the notifications could pose a risk to an individual's health or safety.

Under FIPPA, the following actions are deemed offences:

- The wilful, unauthorized collection, use, or disclosure of Personal Information; and
- The wilful failure to notify the Head of an unauthorized disclosure of Personal Information.

12. INVESTIGATIONS AND BREACH OF POLICY

Complaints and suspected breaches of this policy or FIPPA should be addressed to the Director ATIP who will give notice of the complaint to the General Manager of the responsible department. The Director ATIP, or their delegate, may carry out an investigation and may use and disclose personal information contained in the complaint to employees or service providers of the City as necessary for the purpose of conducting the investigation. Where it is alleged that the breach was by an employee and an investigation is to take place, the Chief Human Resources Officer will be notified and Human Resources may be engaged in the investigation.

After the investigation, a written report will be prepared. The report may contain findings of fact and recommendations aimed at ensuring compliance with this policy and FIPPA.

If required, a copy of the report may be shared on a need-to-know basis to those involved in the investigation.

Breach of this policy, of any procedure created pursuant to it, or of FIPPA may be handled in accordance with the Code of Conduct.

Privacy Breaches that may result in privacy offences will be pursued in accordance with FIPPA.

REFERENCES

Code of Conduct Bylaw No. 12886

Freedom of Information and Protection of Privacy Act

Freedom of Information and Protection of Privacy By-law No. 11451

Freedom of Information and Protection of Privacy Regulation

Records Management By-law No. 9067

RELATED POLICIES

AE-028-01 Code of Conduct

ADMIN-009 Corporate Records and Information Management

APPROVAL AND REVIEW HISTORY:

Version 1 approved by:	City Clerk	12/4/2019
	City Manager	3/20/2020
Version 2 approved by:	City Clerk	10/5/2023
	City Manager	10/13/2023

Next review date **10/13/2026**