CORPORATION OF THE TOWNSHIP OF ESQUIMALT

COUNCIL POLICY

TITLE:	Privacy	NO.	ADMIN-84

Effective Date:	XXXX XX, 2025
Approved by:	Council
Reference:	ADM-25-058
Amends:	New

POLICY

This policy establishes the Township of Esquimalt'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 Township of Esquimalt elected officials, employees, volunteers, agents, and service providers.

This policy does not apply to other Public Bodies differentiated from the Township of Esquimalt under 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 Protection Schedules are legally binding schedules that are 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.

Freedom of Information Request (FOI) is the term used to describe how an individual can exercise their right to request information or records in the custody or control of the Township under section 5 of FIPPA.

Head is the Corporate Officer (or Deputy Corporate Officer in their absence) as designated in the Township of Esquimalt's Freedom of Information Bylaw, 2025, No. 3177 as the Head of the Public Body in accordance with section 77 of FIPPA.

Information sharing is the disclosure of Personal Information from a public body or organization to another party, which then collects and uses that information. This can be a one-way transfer or a reciprocal exchange, a single event or a series of regular transactions.

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, Township employees or agents in relation to the Township'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 Breach Response Procedure outlines the steps in documenting and managing a known or suspected privacy breach.

Proactive Disclosure are records made publicly available on a routine basis.

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).

Security Threat and Risk Assessment (STRA) is the overall activity of assessing and reporting security risks for a new or significantly modified information system to help make well informed risk-based decisions. An STRA also documents risk ratings and planned treatments.

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)

Third Party means a person, entity, business, or a different public body other than the Township of Esquimalt.

COMPLIANCE WITH FIPPA

All persons affiliated with the Township, including elected officials, employees, agents, volunteers, and service providers 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.

ACCOUNTABILITY

Chief Administrative Officer (CAO)

The Chief Administrative Officer is responsible for:

- Ensuring all Employees are given notice of and access to a copy of the most recent version of this policy; and
- Ensuring that the roles and responsibilities listed under this policy are fulfilled.

Director of Corporate Services / Corporate Officer

The Corporate Officer of the Municipality is legally delegated by the Freedom of Information Bylaw, 2025, No. 3177 to fulfill all Township of Esquimalt FIPPA "Head" duties and responsibilities.

The Director of Corporate Services is responsible for:

- Carrying out the duties and responsibilities of the "Head" as set out in FIPPA;
- Developing, implementing, and maintaining the Township's Access to Information and Privacy Program;
- Investigating and responding to Privacy Complaints and Privacy Incidents as per privacy breach procedures;
- Reviewing, commenting, and providing required approvals on PIAs and ISAs and other privacy-related agreements and associated processes;
- Ensuring that employees have access to training and education related to the Township's duties under FIPPA;
- Providing advisory services to employees;
- Maintaining the Township of Esquimalt's PIB;
- Recommending remedial action in response to a breach of this policy or FIPPA;
- Representing the Township before the Office of the Information and Privacy Commissioner (OIPC); and
- Delegating duties assigned under this Privacy Policy.

Manager of Corporate Services / Deputy Corporate Officer
The Deputy Corporate Officer of the Municipality is legally delegated by the Freedom of Information Bylaw, 2025, No. 3177 to perform any duty or exercise any function under FIPPA as designated to the Township of Esquimalt FIPPA "Head".

Freedom of Information Assistant
The FOI Assistant has the following roles and responsibilities:

- Supporting and assisting the Head in their roles and responsibilities;
- Receiving, reviewing, and responding to access requests made under Part 2 of FIPPA;
- Remaining current and knowledgeable about the types of records made routinely available within departments, and remaining aware of circumstances that may require an applicant to file a formal request under FIPPA;
- Remaining current and knowledgeable of the Township's Personal Information holdings;
- Advocating for protection of Personal Information in dealings with Township departments including assisting in the development of Privacy Impact Assessments (PIAs); and
- Consulting with and providing recommendations to the Head in relation to the Township's compliance with FIPPA.

Management
Management is responsible for:

- Complying with the privacy protection requirements in FIPPA and this policy;
- Ensuring employees are familiar with and comply with the privacy protection requirements in FIPPA and this policy;
- Communicating the requirements of FIPPA and this policy to employees in their departments;
- Assigning resources to support compliance with this policy, related procedures, and FIPPA;
- Referring all requests for access to or correction of Personal Information to the FOI & Privacy Team;
- Working collaboratively with the FOI & Privacy Team by responding to requests for records related to FOI requests by conducting comprehensive searches, retrievals and preparations of departmental records and instructing applicable departmental staff to do the same within the prescribed timelines;
- Completing training on FIPPA, including regarding the collection, use, disclosure, storage, retention, and disposal of Personal Information, as appropriate to their work function.
- Ensuring that Personal Information in the custody and control of their department is handled in accordance with FIPPA and this policy;
- Conducting and completing Privacy Impact Assessments (PIAs) prior to implementing new initiatives or significantly changing existing initiatives that involve Personal Information;
- Including the Data Security and Privacy Protection Schedules in all contracts with service providers that involve the collection, use or disclosure of Personal Information;
- Establishing Information Sharing Agreements (ISAs), when required and implementing all required action of ISAs applicable to their department;
- Providing requested assistance to the Freedom of Information Assistant and Head to ensure that the information in the Personal Information Bank (PIB) remains current;

- Working with the FOI & Privacy Team to conduct an investigation into any suspected privacy breach to determine what occurred and what mitigation steps may be required; and
- Reporting actual or reasonably suspected Privacy Incidents to the Head.

Elected Officials / Employees / Agents /Volunteers

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

- Complying with the privacy protection requirements in FIPPA and this policy;
- Completing training on FIPPA, including regarding the collection, use, disclosure, storage, retention, and disposal of Personal Information, as appropriate to their work function.
- Working collaboratively with the FOI & Privacy Team by responding to requests for records related to FOI requests by conducting comprehensive searches, retrievals and preparations of departmental records as assigned by their manager within the prescribed timelines;
- Consulting with their manager, volunteer coordinator and/or Corporate Services regarding the requirements in FIPPA and this policy;
- Referring all requests for access to or correction of Personal Information to the FOI & Privacy Team;
- Reporting actual or reasonably suspected Privacy Incidents to their supervisors and/or the Head;
- Reporting privacy complaints to the Privacy Team as set out in this policy and related procedure documents;
- Including the Data Security and Privacy Protection Schedules in all contracts with service providers that involve the collection, use or disclosure of Personal Information;
- Cooperating with the Head and FOI Assistant in implementing this Privacy policy, related procedures and in complying with FIPPA;

Service Providers

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

COLLECTION

The Township must have legal authority to collect Personal Information. Collection must only occur as permitted under FIPPA and with the completion of a Privacy Impact Assessment (PIA).

Only the minimum amount of Personal Information will be collected and will be accessible to the least number of people to perform required Township functions.

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

NOTICE OF COLLECTION, PURPOSE, AND CONSENT

Personal Information collected by or for the Township must only be collected for an identified Township program or activity except as authorized by statute or regulation.

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.

All forms used to collect Personal Information for providing Township services or other work-related duties, must include a collection statement with the above noted provisions.

When an individual views a collection statement prior to their providing Personal Information, they are deemed to be providing their consent for the collection and use of their Personal Information within the scope of the Notice of Collection.

USE, DISCLOSURE, AND ACCESS

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

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

- For the stated purpose for which it was collected;
- For a use that is consistent with the stated 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.

When the Township wishes to routinely release, proactively disclose or publicly release documents in response to an Access to Records or a Freedom of Information (FOI) request, staff will review the records in consultation with the relevant department and will sever information (including Personal Information) as appropriate according to FIPPA.

For the regular sharing of Personal Information with other organizations such as other government bodies or service providers, Information Sharing Agreements (ISAs) may be required to establish sufficient parameters and security measures around external use and disclosure of Township-held Personal Information.

ACCURACY AND CORRECTION OF PERSONAL INFORMATION

If Personal Information is used by or on behalf of the Township to make a decision about an individual, the Township 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.

STORAGE INSIDE AND OUTSIDE OF CANADA

The Township must make every reasonable effort to ensure Personal Information in the Custody and Control of the Township is stored and/or accessed in Canada.

If Personal Information in the custody or control of the Township is to be stored and/or accessed outside of Canada, a supplemental assessment must be included in the Privacy Impact Assessment (PIA) and approved by the Head. Completion of a formal Security Threat and Risk Assessment (STRA) may also be appropriate.

SECURITY AND PROTECTION

The Township, and all elected officials, employees, agents, and volunteers, must comply with the obligation under FIPPA to protect Personal Information within the Township's custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of Personal Information.
Security arrangements will include appropriate technological, physical, and administrative safeguards.

Completion of a Security Threat and Risk Assessment (STRA) may be undertaken by the Information Technology Department when an initiative involves electronic data collection, use, access, and storage.

RETENTION AND DISPOSITION

The Township will retain and dispose of Personal Information in accordance with the Township's Records Management Policy however the Township 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.

OPENNESS

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

COMPLIANCE REVIEWS AND AUDITS

The Head may conduct compliance reviews and audits in order to assess compliance with FIPPA and will communicate results to the Chief Administrative Officer and the department heads.

BREACHES OF FIPPA AND PRIVACY OFFENCES

If Personal Information or Sensitive Personal Information in the Custody or Control of the Township 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 Head immediately upon discovery. Reporting the suspected breach is mandatory even when the anticipated risks are minimal.

In accordance with the privacy breach response procedure, the Head and/or their delegate will lead an investigation to confirm if a privacy breach has occurred. The supervisor/manager /

department head responsible will work with the FOI & Privacy Team to conduct an investigation to determine what occurred and what mitigation steps may be required.

If a confirmed Privacy Breach poses a risk of significant harm to individuals, the Township is required to provide notifications to the affected individuals and the Office of the Information and Privacy Commissioner (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 Section 65.4, 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.

POLICY BREACHES, COMPLAINTS AND INVESTIGATIONS

Complaints and suspected breaches of this policy or FIPPA should be addressed to the Head who will give notice of the complaint to the Director of the responsible department. The Head, or their delegate, may conduct an investigation and may use and disclose Personal Information contained in the complaint to employees or service providers of the Township 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 Senior Manager of Human Resources will be notified and may be engaged in the investigation. Where it is alleged that the breach was by an Elected Official, Service Provider or Volunteer and an investigation is to take place, the appropriate Department Head, the CAO, or a 3rd party investigator will be notified and 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 ADMIN-80 Council Code of Conduct Policy and/or M-PER-07 Code of Conduct for Employees Policy. Where disciplinary action is warranted as a result of a substantiated complaint, appropriate disciplinary action, up to and including termination of employment (paid or voluntary), will be taken by the Township. Council members may be subject to sanctions. For Service Providers, pursuant to the terms and conditions of a contract for service, the Township may take appropriate action up to and including termination of the contract for service.

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

REFERENCES

Freedom of Information and Protection of Privacy Act
Community Charter
Local Government Act

Freedom of Information Bylaw, 2025, No. 3177
Officers Bylaw, 2011, Amendment Bylaw, 2024, No. 2777

Related Council Policies
ADMIN-42 Records Management
ADMIN-65 Recorded Public Input
ADMIN-77 Imaging of Municipal Records
ADMIN-78 Request for Access to Records, Development Services
ADMIN-80 Council Code of Conduct

Related Management Policies
M-ADM-16 Video Surveillance
M-PER-07 Code of Conduct for Employees