Policy No.: LS-2025-01 - Protection of Personal Information (PIP) Policy

Date Enacted: March 25, 2025

Amended By:

Subject

The Protection of Personal Information Policy ("PIP Policy") for the Municipality of Leamington.

Purpose

The purpose of this policy is to ensure that the Municipality of Leamington (the "Municipality") meets or exceeds its legislated responsibilities in the management of personal information as set out in the Mmunicipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56 and other applicable legislation.

Scope

This policy applies to all full-time Employees including those who are members of a bargaining unit, part-time, casual, and seasonal, contract and student positions; volunteers; members of Council and members of local boards and committees.

Definitions

Act means the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56.

Clerk means the Clerk appointed by the Council of The Corporation of the Municipality of Leamington.

Collection means the gathering or obtaining Personal Information from any source (including verbally or in written or electronic format).

Consent (to the Collection, Use or Disclosure of Personal Information) means freely given, specific, informed, and unambiguous indication of the information subject's wishes to collect or process their Personal Information.

Council means the Council of the Municipality.

Disclosure (of Personal Information) means showing, sending, or giving some other organization, government, contractor, or individual Personal Information.

Disposition (of records) means the final action taken upon the expiration of a record's retention period, in accordance with the Municipality's Records Retention By-law, provided the record is not subject to a legal hold.

Employee means an employee of the Municipality including but not limited to those who are employed pursuant to a contract, casual and seasonal, part-time employees; co-op students and volunteers

Municipality means The Corporation of The Corporation of the Municipality of Leamington.

Personal information means recorded information about an identifiable individual, such as (but not limited to):

- Names
- Residential street addresses
- Telephone numbers
- Email addresses
- Marital/relationship/family status
- Views and opinions
- Opinions of others about the individual
- injuries, diagnosis, and treatment).
- Descriptions of activities/location of Person/use of property
- Images of Persons
- Financial activities (payments and purchases)
- Medical information (e.g. medical history, health status, description of

Personal Information Bank (PIB) means a Collection of Personal Information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual.

Privacy means a set of interests and rights that an individual has regarding their ability to control the Collection, Use, Disclosure, and retention of their own Personal Information that is in custody or control of another. Privacy is not an absolute right in all situations. Personal information may be Collected, Used, Disclosed, or retained without the Consent of individuals where specific legislation permits.

Privacy Breach means the use or disclosure of Personal Information or records containing Personal Information in violation of Sections 31 or 32 of the Act or other applicable legislation.

Privacy Impact Assessment (PIA) means a comprehensive assessment of a project

or a system that identifies the impact that the project or system might have on the Privacy of individuals, and sets out recommendations for managing, minimizing, or eliminating that impact.

Program means Privacy Protection Management Program.

Security Safeguards means physical, technical administrative and organizational measures put in place to protect the security, value, or integrity of Personal Information.

Third Party means any outside individual (such as a consultant or contractor), a business or an organization that provides a service to, or acts on behalf of, the Municipality.

Use (of Personal Information) means using Personal Information to carry out the Municipality's purpose for collecting the information.

POLICY

1. The Municipality is committed to protecting the Privacy of individuals and ensuring the confidentiality and security of the Personal Information it Collects, Uses, and Discloses.

2. Underlying all privacy regimes are fundamental principles. The Municipality adopts the 10 principles known as the Fair Information Principles developed by the Canadian Standards Association as guiding principles for the Collection, Use, and Disclosure of Personal Information (copy of which is attached to this Policy as Appendix "A"). Adherence to these principles assists the Municipality in achieving positive outcomes by how it manages and protects Personal Information in its custody and/or under its control.

   Principle 1 - Accountability

   The Municipality takes responsibility for the Personal Information under its control, including Personal Information that is collected on behalf of the Municipality and any Personal Information transferred to Third Parties for processing and designates an individual responsible for overseeing the Municipality's Program.

   To comply with this principle the Municipality will:

   - designate the Clerk, the "Chief Privacy Officer" who is responsible for overseeing the development, implementation, monitoring, assessment and review of Personal Information management policies and practices.
   - implement a Privacy Protection Management Program to comply with the applicable legislation and 10 Fair Information Principles.
   - Train staff in the Municipality's privacy policies and practices.
   - develop information to communicate the Municipality's privacy policies and

procedures.

Principle 2 - Identifying Purposes

The Municipality will identify the purpose(s) for Collecting Personal Information and will inform individuals why and/or how the Personal Information is being Used or Disclosed, before or at the time of Collection as set out in the Act.

To comply with this principle the Municipality will:

- provide notices of Collection of Personal Information before or at the time of Collection. Depending on the way Personal Information is Collected, this can be done orally or in writing. The purpose will be communicated in a manner that is clear and can be reasonably understood. A written notice, at a minimum, will include the legal authority for the Collection, the principle purpose for which the Personal Information is intended to be used, and the title and contact information of the Chief Privacy Officer who can answer questions about the Collection.
- create an inventory of Personal Information holdings (Personal Information Banks).
- ensure that the Collection of Personal Information is necessary to fulfill the identified purpose.
- ensure that purposes are limited and reasonably appropriate.
- inform the individuals when using Personal Information for a new purpose not previously identified and obtain their Consent, prior to its Use.
- should the Municipality propose to Use or Disclose Personal Information that has been collected for a purpose not previously identified, the individual's Consent is first obtained except in those circumstances set out in the Act.

Principle 3 - Consent

The Municipality will obtain meaningful Consent for the Collection, Use and Disclosure of Personal Information, except where inappropriate or otherwise permitted by legislation.

To comply with this principle the Municipality will:

- seek Consent for the Use and Disclosure of Personal Information at the time of Collection. In some cases, Consent may be sought after the information has been collected, but before Use.
- avoid making Consent a condition for delivering services, unless the Collection, Use or Disclosure of Personal Information is necessary to provide the service.
- make a reasonable effort to make Consent meaningful so that individuals can reasonably understand how their information will be Used and/or Disclosed.
- consider the sensitivity of information and circumstances in determining the

form of Consent – express or implied.
- provide individuals with a mechanism to withdraw their Consent, subject to legal obligations and reasonable notice.

Principle 4 - Limiting Collection

The Municipality will limit the Collection of Personal Information to what is necessary to fulfill the purpose identified by the Municipality.

To comply with this principle the Municipality will:

- be transparent about the purposes of collecting Personal Information.
- collect Personal information by equitable and lawful means.
- limit the amount and types of Personal Information it collects to what is necessary for the identified purposes.
- maintain a Personal Information Bank and review/audit it regularly to ensure that Personal Information is Used for the identified purpose(s).

Principle 5 - Limiting Use, Disclosure and Retention

The Municipality will not Use or Disclose Personal Information for purposes other than those for which it was collected, except with the Consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of these purposes.

To comply with this principle the Municipality will:

- Collect, Use, or Disclose Personal Information only for purposes that a reasonable person would consider appropriate in the circumstances.
- obtain Consent if Use or Disclosure of Personal Information for a new purpose is considered;
- create and review regularly an inventory of Personal Information (Personal Information Banks);
- put guidelines and procedures in place for retaining and destroying Personal Information; and
- Personal Information will be Disposed of once it no longer fulfills its identified purpose. Disposal will be done in a secure manner based on the nature and sensitivity of the Personal Information and in accordance with the Municipality's Records Retention Schedule.

Principle 6 - Accuracy

The Municipality will maintain Personal Information as accurate, complete, and up to date as is necessary for the purposes for which it is to be Used.

To comply with this principle the Municipality will:

- put protocols in place to keep information sufficiently accurate, complete, and up to date, to minimize the possibility that inaccurate Personal Information is Used to make a decision about the individual or when disclosing the Personal Information about an individual to a Third Party.
- provide avenues for individuals to supply/update information to avoid inaccurate Personal Information from being Used to make a decision about them.

Principle 7 - Safeguards

The Municipality will protect Personal Information through appropriate Security Safeguards relative to the sensitivity of the information.

To comply with this principle the Municipality will:

- put in place Security Safeguards to protect Personal Information throughout its entire lifecycle (against loss, theft, as well and unauthorized Collection, Use, Disclosure, copying, modification, and Disposition) regardless of the format in which it is held. Regular reviews of safeguards will be conducted.
- provide Employee's and or Third Party's access to Personal Information only when they require it to perform a business-related activity/function that is consistent with the purpose for which the Personal Information was collected.
- develop and implement training as well as awareness tools addressing Personal Information protection methods.

Principle 8 - Openness

The Municipality will make information about its policies and practices relating to the management of Personal Information publicly and readily available.

To comply with this principle the Municipality will:

- make the following information available proactively and upon request.
  - the title and contact information of the Chief Privacy Officer or an alternate Employee, who will be able to explain Personal Information policies and practices or answer questions about the purpose for collecting Personal Information.
  - the process an individual can follow to gain access to their Personal Information and the title and contact information of the Chief Privacy Officer or an alternate Employee they can contact to make such a request.
  - information that explains the Municipality's Personal Information policies, practices and/or procedures.
  - the process for making a complaint about the Municipality's Personal Information practices.

- have protocols for Privacy Breach notification of affected individuals in place.
- make information about the Municipality's privacy practices easily understandable for its stakeholders.

Principal 9 – Individual Access

Upon request, an individual will be informed of the existence, Use, and Disclosure of their Personal Information and be given access to that information. An individual will be provided with an opportunity to challenge the accuracy and completeness of the information and have it amended as appropriate.

To comply with this principle the Municipality will:

- have processes in place for providing individuals with information about the Personal Information the Municipality holds about them, as well as a process for correcting individuals Personal Information, when requested or discovered to be inaccurate or incomplete.
- provide reasonable assistance to individuals with preparing Personal Information access requests and understanding information about them that the Municipality holds (where necessary).
- provide individuals with access to their Personal Information, as permitted by the Act.

Principle 10 - Challenging Compliance

The Municipality will provide individuals with avenues to challenge its Personal Information handling practices and take reasonable steps to address these challenges.

To comply with this principle the Municipality will:

- put protocols in place to receive, investigate and respond to complaints or inquiries about its practices of handling Personal Information;
- take appropriate measures to correct information handling practices, if found inadequate;
- inform complainants about other avenues of recourse, where appropriate.

3. The Municipality's Program will include the following elements:

3.1 Organizational Commitment demonstrated by:

- Council and Senior Management's endorsement of the Program.
- Resources allocated to oversee and monitor the Municipality's compliance, so that Privacy Protection is built into functions involving the Use of Personal Information, including policies, programs, services, agreements and contracts, information technology systems and

software, communications, etc.

3.2 Program controls, which include (but are not limited to):

- Personal Information inventory (Personal Information Banks);
- policies, procedures, and guidelines;
- risk assessment tools (e.g., Privacy Impact Assessments);
- training, education and awareness;
- Privacy Breach and incident management protocols;
- service provider management;
- external communications (e.g., notices of Collection; protocols for Privacy Breach notifications, Third Party notification, obtaining Consent, etc.)

3.3 Ongoing assessment and revision of the Program components.

4. Accountability

Council and Senior Management:

- endorse and promote compliance with the Program and its controls within the departments/divisions they manage.
- ensure that Privacy protection measures are integrated into the development, implementation, evaluation, and reporting activities of services, programs and projects within their departments/divisions.
- support the Program with resources that it needs to succeed.

Clerk or Designate:

- oversee the Program and Municipality's compliance with MFIPPA, other legislation setting forth Privacy protection requirements, as well as the Program and its controls.
- monitor compliance with the Program.
- coordinate the development and implementation of the Program controls.
- advise municipal departments on building Privacy protection measures into activities, services, programs and projects that involve the Use of Personal Information. Such measures may include but are not limited to procedures, guidelines, contracts, by-laws, information technology systems or software, and communications.
- coordinate the development and implementation of Program monitoring, auditing, and revision procedures.

Municipal Employees

- comply with this Policy and associated procedures (including department specific privacy procedures and guidelines).

- collaborate with Employees responsible for the Program coordination in developing, implementing, and monitoring the Program and its controls and tools.
- participate in Privacy protection training and awareness events.

Third Parties

- comply with this policy and associated procedures and other Privacy protection instruments that may be developed from time to time.
- cooperate with the Clerk and/or Employees to complete PIA's, where required, and comply with any recommendations provided in the PIA report.
- follow procedures, guidelines, or other instruments as they may be developed from time to time, for the specific services provided by them.
- if required, complete privacy training specific to the services provided by them.

COMPLIANCE:

In cases of policy violation, the Municipality may investigate and determine appropriate corrective action.