CORPORATE POLICY

Policy Title: **Privacy Protection Program Framework**
Policy Category: **Administration Policy**
Policy No.: A-039
Department: Corporate Services
Approval Date: June 12, 2023
Revision Date: N/A
Author: Natalia Chebel, Justice Marfo
Attachments:
Related Documents/Legislation:
Municipal Freedom of Information and Protection of Privacy Act, as amended
Personal Health Information Protection Act, as ameded
Information Security Policy
Records Management Policy

Key Word(s): privacy protection, records, information security

POLICY STATEMENT:

The City of Waterloo is committed to protecting the privacy rights of individuals and ensuring the confidentiality and security of the personal information it collects. The City of Waterloo will ensure adherence to the privacy protection provisions of the *Municipal Freedom of Information and Protection of Privacy* Act (MFIPPA) (as amended), *Personal Health Information and Protection of Privacy Act (PHIPPA*) (as amended) and other applicable legislation.

The City of Waterloo will:

- ensure that privacy protection measures are embedded in all City programs, applications, technology and technology architecture, projects and etc.;
- be transparent about how personal information is managed, and
- establish privacy protection procedures and guidelines and the privacy protection training and awareness program to implement this policy.

PURPOSE:

The purpose of this policy is to ensure that:

- the City of Waterloo meets its legislated responsibilities in the management of personal information;

Mandatory Policy, *Municipal Act*: No
Policy Administration Team, Review Date May 11, 2023
Corporate Management Team, Review Date May 17, 2023

- principles and components of the Privacy Protection Program are identified;
- roles and responsibilities for the protection of personal information managed by the City are assigned;
- privacy principles are integrated into all new and modified programs, technologies and activities involving personal information.

This Policy should be read in conjunction with *MFIPPA, PHIPPA* and other applicable legislation, policies, procedure, guidelines and other instruments that are established from time to time.

DEFINITIONS:

City means the Corporation of City of Waterloo.

Clerk means the City Clerk of the Corporation of the City of Waterloo.

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 process their personal information. This indication can be a statement or a clear affirmative action.

> **Express consent** means consent that has been clearly and unmistakably given. Express consent may be explicitly provided, either orally or in writing.
>
> **Implied Consent** (to the collection, use or disclosure of personal information) means consent that is not given explicitly, but which can be inferred based on the individual's actions and the facts of a particular situation.
>
> **Meaningful consent** means that individuals who are consenting to the collection, use and disclosure of personal information understand the nature, purpose and consequences of what they are consenting to.

Contractor is any person(s) or firm(s) that provides goods and/or services to the City under terms specified in a contract or other agreement and is not paid through the City's payroll.

Disclosure (of personal information) means releasing or making the information available to an individual or organization.

Disposition (of records) means the final action taken upon the expiration of a record's retention period provided the record is not subject to a record hold.

Employee is a person who performs work (also known as worker) or supplies services for monetary compensation (as defined under the Occupational Health and Safety Act (OHSA)). It also includes all secondary or post-secondary students who perform work or

supply services for monetary compensation or for no monetary compensation under a work experience program operated by or approved by a secondary or post-secondary institution.

Management: for the purpose of this policy and related procedures, guidelines and forms, the term includes employees with the titles of *Manager, Assistant Deputy Chief, Deputy Chief, Director, Fire Chief, Commissioner, CAO or any equivalents to such titles.*

Person means an individual or a business, government or other entity.

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

- Names
- Residential street addresses
- Telephone numbers
- Email addresses
- Gender identifiers(use of pronouns, collection of gender based data)
- Marital/relationship/family status
- Views and opinions
- Opinions of others about the individual
- Descriptions of activities/location of person/use of property
- Images of persons
- Images of use of property (e.g. photos of the inside of homes)
- Financial activities (payments and purchases)
- Medical information (e.g. medical history, health status, description of injuries, diagnosis, and treatment).

Personal Information Bank 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 the custody or control of a third party. 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 an incident involving unauthorized collection, retention, use or disclosure of personal information in the custody and under the control of the City.

Privacy Impact Assessment (PIA): 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 program.

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

Use (of personal information) means viewing or dealing with the information in a manner that does not include disclosing it.

Volunteer is anyone who, without compensation or expectation of compensation, performs a task at the direction of and on behalf of the City.

SCOPE:

This Policy applies to employees, members of Council, contractors and volunteers and to any other persons providing programs or services on behalf of the City.

POLICY COMMUNICATION:

This policy will be made available to employee through the City's website, intranet and training/awareness sessions. Procedures, protocols and other tools associated with this policy will also be communicated to City employee, contractors and members of Council via training and awareness events.

POLICY:

1. The City will adopt 10 principles of privacy protection developed by the Canadian Standards Association, and known as *Fair Information Practices*:

    1.1 Accountability

The City takes responsibility for the personal information it collects, including personal information that is collected for the City by third parties and any personal information transferred to a third party for processing.

To comply with this principle the City will:

- implement a Privacy Management Program to comply with the applicable legislation and 10 fair information principles;
- make the City Clerk (or designate) responsible for overseeing the Privacy Management Program compliance, and
- develop, implement, monitor, assess and review of personal information management policies and practices.

1.2 Identifying Purposes

The City will identify purposes for collecting personal information and will inform individuals why personal information is needed, before or at the time of collection.

To comply with this principle the City 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. A written notice, at a minimum, will include the legal authority for the collection, the principal purposes for which the personal information is intended to be used, and the title and contact information of a City employee who can answer questions about the collection;
- document purposes of collection of personal information holdings (Personal Information Banks or PIB's);
- ensure that the collection of personal information is necessary to fulfill the identified purpose;
- ensure that purposes are limited and reasonably appropriate, and
- inform the individuals when using personal information for a new purpose not previously identified and obtain their consent, prior to its use.

1.3 Consent

The City 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 City 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, and
- provide individuals with a mechanism to withdraw their consent, subject to legal obligations and a reasonable notice.

1.4 Limiting Collection

The City will limit the collection of personal information to what is necessary to fulfill an identified purpose.

To comply with this principle the City will:

- be transparent about the purposes of collecting personal information;

- collect personal information by equitable and lawful means;
- limit the amount an types of information it collects to what is necessary for the identified purposes, and
- maintain a PIB and review/audit it regularly to ensure that personal information is used for the identified purpose(s).

1.5 Limiting Use, Retention and Disclosure

The City 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 City 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
- retention and disposition guidelines of personal information will Dispose of personal information 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

1.6 Accuracy

The City 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 City will:

- put protocols in place to keep information sufficiently accurate, complete and up-to-date, to minimize the possibility that inaccurate information is used to make a decision about the individual or when disclosing information about an individual to a third party;
- update personal information routinely ONLY when such a process is necessary to fulfil the purposes for which the information was collected, and
- provide avenues for individual to supply/update information to avoid inaccurate personal information from being used to make a decision about them.

1.7 Safeguards

The City will protect personal information through appropriate security safeguards relative to the sensitivity of the information.

To comply with this principle the City will:

- put in place security safeguards to protect personal information throughout its entire lifecycle (against loss, theft, as well and unauthorized collection, access, disclosure, copying, use, modification, and disposition) regardless of the format in which it is held. Regular reviews of safeguards will be conducted;
- provide City Employee's and or Contractor's access to personal information only when they require it to perform a business related activity/function, and
- develop and implement employee, volunteer, contractor and Councillor training as well as awareness tools addressing personal information protection methods.

1.8 Openness

The City 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 City will:

- make the following information available proactively and upon request:
    - the title and contact information of a employee member, 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 employee an individual can contact to make such a request;
    - information that explains the City's personal information procedures and practices, and
    - the process for making a complaint about the City's personal information practices.
- have protocols for privacy breach notification of affected individuals in place, and
- make information about the City's privacy practices easily understandable for its stakeholders.

1.9 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 City will:

- have processes in place for providing individuals with access to information the City 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 City holds (where necessary), and
- provide individuals with access to their personal information, as permitted by legislation.

1.10 Challenging compliance

The City will provide individuals with avenues of challenging its personal information handling practices and take reasonable steps to address these challenges.

To comply with this principle the City 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.

2. The City's Privacy Management Program will include the following elements:

2.1. Organizational Commitment demonstrated by:
- the management endorsement of the Program;
- employee resources allocated to oversee and monitor the City's compliance, so that privacy protection is built into functions involving the use of personal information, including policies, programs, agreements and contracts, IT systems, communications, etc.

2.2. 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 Assessment Procedure);
- training, education and awareness;
- breach and incident management protocols;
- service provider management;
- external communications (e.g., notices of collection; protocols for breach notifications, third party notification, obtaining consent, etc.)

2.3. Ongoing assessment and revision of the program components.

3. Accountabilities

City 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:

- Oversees the Program and City's compliance with MFIPPA, other legislation setting forth privacy protection requirements, as well as the Program and its controls.

The Clerk will delegate the responsibility to develop and coordinate the Program and its controls to employee(s) who will:

- provide support to the City Clerk in monitoring compliance with the Program;
- coordinate the development and implementation of the Program controls;
- advise City departments/divisions on building privacy protection measures into activities of 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, IT systems, and communications;
- coordinate the development and implementation of Program monitoring, auditing and revision procedures.

City Employees and Volunteers

- Comply with this Policy and associated procedures (including department/division 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.

Contractors

- Comply with this Policy and associated procedures and other privacy protection instruments that may be developed from time to time.
- Cooperate with City 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 City may investigate and determine appropriate corrective action.