City of Mississauga

Corporate Policy & Procedure

Policy Title: **Privacy**

Policy Number: 03-02-12

Section**: Corporate Administration**	Subsection**: Records Management**
Effective Date: **November 30, 2023**	Last Review Date: **N/A**
Approved by:	Owner Division/Contact**:**
Leadership Team	**Deputy Clerk, Legislative Services, Corporate Services**

Policy Statement

The City is committed to the protection of privacy as it collects, uses, retains, discloses and disposes of Personal Information in the course of meeting its statutory duties and responsibilities.

Purpose

This policy provides guidance on protecting Personal Information in the custody or under the control of the City.

Scope

This policy applies to all persons who collect, use, retain, disclose and/or dispose of Personal Information on behalf of the City, including employees, contractors, agents, elected officials, citizen members of committees and volunteers.

Refer to Corporate Policy and Procedure – Accessing City Information regarding access to Records and information retained by the City.

Refer to Corporate Policy and Procedure – 03-02-07 – Access to Employee Records for information on access to the City's personnel Records.

Refer to the Freedom of Information and Protection of Privacy Manual, available from the Access and Privacy Unit, for in-depth information related to the City's privacy practices.

Legislative Requirements

The City is required to comply with all applicable privacy provisions in the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), and any other applicable legislation, including the *Personal Health Information Protection Act* (PHIPA).

Definitions

For the purposes of this policy:

“Personal Information” or “PI”, also known as personally identifiable information (PII) or personal data, is information relating to an identified or identifiable individual in their personal capacity. Personal Information includes but is not limited to:

- Race, national or ethnic origin, religion, age, gender, marital or family status
- Education, medical, criminal or employment history
- An individual’s financial transactions
- Identifying numbers and addresses, including personal email addresses
- Biometric information, including fingerprints and facial recognition
- An individual's personal opinions except where they relate to another individual, and
- Correspondence sent to the City that is implicitly or explicitly of a private or confidential nature (and replies to the correspondence, if the replies would reveal the nature of the original correspondence)

  For greater clarity, information is about an identifiable individual if:
  - It is about the individual in a personal capacity; that is, it reveals something of a personal nature about the individual, and
  - It is reasonable to expect that an individual could be identified through the use of that information, alone or in combination with other information

  Notes:
  1. Personal Information does not include an individual’s name, work address, work telephone number or position when acting in their business or professional capacity.
  2. Personal Information does not include information about an individual who has been dead for more than thirty years.

“Privacy Breach” means any collection, use, retention, disclosure or disposal of Personal Information in contravention of legislative requirements, contractual requirements and/or City policy.

“Personal Information Bank” or “PIB” is a description of Personal Information that the City maintains and uses in delivering programs and services (note that MFIPPA requires the City to make an index of its PIBs available to the public).

“Privacy Impact Assessment” or “PIA” means a risk management process that helps the City ensure legislative compliance, implement appropriate security measures and identify the impacts its programs, services, projects, technologies and/or applications will have on individuals’ privacy.

“Record” means recorded information regardless of physical form or characteristics, whether in printed or electronic form, that is made or received by the City to conduct its business and may include, but is not limited to, correspondence, memoranda, minutes, books, plans, maps, drawings, email, and system use/access logs.

Accountability

Directors

Directors are accountable for:

- Ensuring all applicable managers/supervisors are aware of this policy and of any subsequent revisions
- Ensuring compliance with this policy in conjunction with any related procedures, and
- Ensuring the security of Personal Information in their custody or under their control (including Personal Information stored in a database)

Director, Legislative Services & City Clerk

The City Clerk is accountable for:

- Performing the duties of head of the institution, as required by MFIPPA
- Ensuring an index of PIBs is available for public inspection, and
- Ensuring Privacy Breaches are investigated and appropriately mitigated

Director, Information Technology & Chief Information Officer (CIO)

The CIO is accountable for ensuring that technologies that are developed or acquired by the City, along with technology-related services, adequately maintain the confidentiality, integrity and availability of Personal Information using appropriate security assessments and security controls.

Manager, Employee Health Services

The Manager of Employee Health Services is accountable for performing the duties of Health Information Custodian (HIC), as required by PHIPA.

Managers/Supervisors

Managers/supervisors with staff, contractors, agents and/or volunteers under their supervision who are responsible for the custody, control and access to Personal Information are accountable for:

- Ensuring staff in their respective work units are aware of and trained on this policy and any associated procedures, as well as any subsequent revisions, with respect to their specific job function
- Ensuring that access to and use of Personal Information are restricted to those having a legitimate business need for the information, and
- Ensuring that the Access and Privacy Unit has an up-to-date PIB(s) for their respective work units

Access and Privacy Unit

Access and Privacy Unit staff, Legislative Services Division, are responsible for:

- Providing guidance and support to assist employees at all levels in developing appropriate practices related to privacy

- Supporting employees at all levels, as required, in completing PIAs and providing recommendations to mitigate any privacy risks identified in the assessments
- Developing and supporting privacy training for employees, contractors, agents, elected officials, citizen members of committees, and volunteers, as appropriate
- Managing the PIB index, ensuring that PIBs are accurate and up-to-date and publishing PIBs on behalf of the City, and
- Investigating privacy complaints/incidents and responding to Privacy Breaches with the support of Legal Services, Internal Audit and/or Information Technology, as appropriate

Employees

Employees are responsible for:

- Being familiar with legislative requirements pertaining to privacy in relation to their particular job function and completing privacy-related training, as appropriate
- Complying with this policy and any associated procedures with respect to the Personal Information they collect, use, disclose, retain and/or destroy
- Completing Privacy Impact Assessments as outlined in this policy, and
- Reporting privacy complaints, incidents and breaches to the Access and Privacy Unit at privacy.info@mississauga.ca

Contractors, Agents, Elected Officials, Citizen Members of Committees and Volunteers

Contractors, agents, elected officials, citizen members of committees and volunteers are responsible for:

- Being familiar with legislative requirements pertaining to privacy in relation to their particular duties and attending privacy-related training, as appropriate
- Complying with this policy and any associated procedures with respect to the Personal Information they collect, use, disclose, retain and/or destroy, and
- Reporting privacy complaints, incidents and breaches

Fair Information Principles

The City adheres to the Canadian Standards Association's 10 fair information principles:

1. Accountability

Under MFIPPA, the head of the institution (City) is accountable for ensuring Personal Information under the City's control is protected, and that access to Personal Information is provided only to persons with a right of access. Council has designated the City Clerk as the head through By-Law 0053-91, as amended from time to time.

All persons acting on behalf of the City are responsible for protecting Personal Information in their immediate control.

2. Identifying Purpose

All persons acting on behalf of the City must identify the purpose(s) for which Personal Information is collected in regards to a City program, service or activity and notify affected

individuals of these purpose(s), as well as any other information required by law, at or before the time the Personal Information is collected.

The specific purpose for collecting Personal Information should be defined as clearly as possible to ensure individuals understand how their information will be used or disclosed.

3. Consent

The knowledge, and in some cases the consent, of an individual is required before or at the time of the collection of Personal Information. Affected individuals must be informed in a meaningful way of the purpose(s) of the collection, use, retention and disclosure of Personal Information (i.e. the affected person should understand the how their Personal Information will be used), except where otherwise permitted by law. City programs, services and activities that involve the collection of Personal Information, whether recorded or unrecorded, must include a (written or verbal) notice of collection of Personal Information.

Individuals have the right to withdraw consent at any time, although withdrawal of consent may affect access to City programs, services and activities.

4. Limiting Collection

All persons acting on behalf of the City must limit the collection of Personal Information to that which is necessary to deliver City programs, services and activities. Personal Information must only be collected through fair and lawful means.

5. Limiting Use, Retention and Disclosure

All persons acting on behalf of the City must not use, retain or disclose Personal Information for purposes other than those for which it was collected, except with the consent of the affected individual(s) or as authorized or required by law. Personal Information must be retained in accordance with the applicable Records Retention Schedule contained in the Records Retention By-law 0097-2017, as amended from time to time.

Requests from Individuals to delete/destroy their Personal Information may be actioned if:

- The Personal Information is not required to comply with a legal ruling or obligation (such as MFIPPA and Records Retention By-law 0097-2017 requirements), and
- The City is able to do so without undue hardship

6. Accuracy of Personal Information

All persons acting on behalf of the City must take reasonable steps to only use Personal Information that is accurate, complete and as up-to-date as possible in order to fulfill the specified purposes for its collection, use, disclosure and retention.

7. Safeguarding Personal Information

All persons acting on behalf of the City must ensure that Personal Information is secured and protected from unauthorized access, use, disclosure and inadvertent destruction by adhering to safeguards appropriate to the format and sensitivity of the information.

8. Access to and Correction of Personal Information

Upon request, the City will allow an individual to access their own Personal Information, subject to any legislative limitations and/or restrictions.

An individual has the right to challenge the accuracy and completeness of Personal Information in City Records and to request that the Personal Information be amended as appropriate or, if the City declines to amend the information, to have a letter/statement of disagreement retained on the file. Any individual to whom the disclosure of the Personal Information has been granted in the year preceding a correction has the right to be notified of the correction/statement.

9. Openness and Transparency

The City makes its policies and practices relating to the collection, use, disclosure, retention and destruction of Personal Information available to the public. Where possible, information pertaining to privacy protection shall be published to the City's website, where information is unpublished, it shall be disclosed upon request.

10. Challenging Compliance

If an individual believes that the City is not in compliance with the fair information principles, they may contact the Access and Privacy office, who will ensure that the concerns are investigated. If a complaint is found to be justified, the City will take appropriate measures, including, if necessary, amending its policies and procedures. Individuals also have the right to lodge (or escalate) a complaint to the Office of the Information and Privacy Commissioner of Ontario.

Privacy Impact Assessments (PIAs)

The purpose of a PIA is to identify privacy-related risks and to articulate recommendations on:

- Meeting legal, regulatory and policy obligations, and
- Appropriate risk mitigation

Where a City program, service, activity or technology collects, uses, retains, discloses or destroys Personal Information, a PIA must be completed. As required, the Access and Privacy Office supports PIAs for the:

- Review of an existing program, service, activity, project, technology or application
- Implementation of changes to an existing program, service, activity, project, technology or application
- Implementation of a new use of an existing technology or application, and
- Implementation of a new program, service, activity, project, technology or application

The City employs a range of tactics for the completion of a PIA. Generally, the PIA process involves:

- The collection, documentation and analysis of relevant information
- A qualitative assessment of potential risk(s)
- The generation of a risk rating (sometimes expressed as a heat map)

- Recommendations that employees could use to mitigate risk(s) associated with their program, service or technology, and
- Evaluation of implemented risk mitigation strategies by the Access and Privacy Office to determine the effectiveness and to generate a final risk rating

Personal Information Bank (PIB) Index

MFIPPA requires the City to keep an index of all PIBs in its custody or control. This index must contain the following in respect of each PIB:

1. Its name and location
2. The legal authority for its establishment
3. The types of Personal Information maintained in it
4. How the Personal Information is used on a regular basis
5. To whom the Personal Information is disclosed on a regular basis
6. The categories of individuals about whom Personal Information is maintained, and
7. The policies and practices applicable to the retention and disposal of the Personal Information

Upon request, the Access and Privacy Unit will make the PIB index available to the public for inspection.

Privacy Breaches

Any person acting on behalf of the City who believes a Privacy Breach may have occurred must report it to the Access and Privacy Unit at privacy.info@mississauga.ca. The Access and Privacy Unit investigates all privacy concerns and incidents.

If a Privacy Breach is confirmed, the Access and Privacy Unit, supported by subject matter experts, Legal Services, Internal Audit, IT Security, Security Services and Strategic Communications and Initiatives, as appropriate, will take action to ensure that:

- The Privacy Breach is contained
- Individuals affected by the Privacy Breach are notified
- Appropriate mitigation measures are implemented
- The Privacy Breach is reported to senior management, Council and/or the appropriate authorities, as applicable, and
- Remedial strategies, procedures and/or training are implemented, as appropriate, to reduce the likelihood of similar Privacy Breaches in the future

Compliance

Employees who fail to comply with this policy will be subject to appropriate disciplinary action, up to and including termination of employment. Unionized employees will be disciplined subject to any applicable provisions of their particular collective agreement.

Non-compliance by persons other than employees will be addressed, as appropriate, in accordance with the relevant contract, agreement and/or terms of reference.

Persons who contravene MFIPPA may be charged by the Attorney General under the authority of the Act, and if convicted, fined up to $5,000.

Revision History

Reference	Description
LT – 2023 11 30	Replaces Corporate Policy and Procedure - 03-02-08 - Freedom of Information and Protection of Privacy (now rescinded). See also Accessing City Information policy #03-02-13.