SECTION:	ARCHIVES, RECORDS & PRIVACY
DEPARTMENT/DIVISION:	CITY MANAGER'S OFFICE / OFFICE OF THE CITY CLERK
SUBJECT:	**ACCESS AND PRIVACY**

POLICY STATEMENT

The Corporation of the City of Thunder Bay (the "City") is committed to protecting the privacy of Personal Information of individuals, while also providing members of the public with access to information.

PURPOSE

This policy outlines how the City complies with legislative obligations with respect to access to information and protection of privacy in accordance with the Ontario *Municipal Freedom of Information and Protection of Privacy Act* ("MFIPPA").

This policy summarizes roles and responsibilities related to:

- access to information; and
- protection of Personal Information, with respect to the collection, use, disclosure, retention and disposition of Personal Information.

This policy is not meant to provide legal advice. This policy should be read in conjunction with the current law and other relevant documents of the City.

SCOPE

This policy applies to corporate records and Personal Information in the custody or control of the City.

This policy applies to all City employees, contractors, volunteers, third party service providers and any other persons providing services or programs on behalf of the City.

This policy also applies to records and information of the Office of the Mayor and members of Council that are created and used for the purpose of carrying out business of the City.

This policy does not apply to Personal Health Information that falls under the purview of a health information custodian as defined in the Ontario *Personal Health Information Protection Act, 2004* ("PHIPA"), such as Pioneer Ridge/Jasper Place and Superior North Emergency Medical Services. However, the Director – Legislative Services & City Clerk works in partnership and may be consulted on privacy matters that impact health information custodians.

POLICY

Access to Information

The City is committed to providing information to the public.
City records, which are in the custody or control of the City can be accessed through:

1. **Public Record Request:** Authorized City employees can provide access to a record that is created or maintained for a public purpose.
2. **Routine Disclosure:** Authorized City employees can provide access to a record that has a departmental routine disclosure plan approved by the Director – Legislative Services & City Clerk or delegated employees.
3. **Freedom of Information (FOI):** A formal access to information request in accordance with MFIPPA.

The City recognizes an individual's right of access to information and the correction of Personal Information. City staff must verify the identity of individuals requesting their own Personal Information.

The City has a corporate policy for Records Management (03-06-01) and values the role that records management plays in access to information. Employees must ensure that a timely response is provided and a reasonable search is conducted for requesters, including when assisting with responding to Freedom of Information requests.

It is an offence to:

- wilfully disclose Personal Information in contravention of MFIPPA;
- wilfully maintain a Personal Information bank that contravenes MFIPPA; or
- alter, conceal or destroy a record, or cause any other person to do so, with the intention of denying a right under MFIPPA to access the record or the information contained in the record.

Protection of Personal Information

Collection Notification:

MFIPPA provides when Personal Information may be collected and the requirements associated with the collection.

1. Personal Information will be directly collected from the individual, with limited authorized exceptions.
2. An attempt to ensure the accuracy of the Personal Information will be made.
3. Collection of Personal Information will be limited to what is necessary for the administration of City services, programs or business.
4. Prior to the collection of Personal Information, and as prescribed by MFIPPA, the following notice will be provided:
    - the legal authority for the collection;
    - the purpose(s) for which the Personal Information is intended to be used; and

- the contact information (title, business address and business telephone number) for the individual in the business unit who can answer questions about the collection of the Personal Information.

5. Preferably, the notice of collection will be in written format, however, where impractical verbal notice of collection may be used.
6. Notice of collection statements will be reviewed by the responsible business unit periodically to ensure accuracy.

Use and Disclosure of Personal Information:

Personal Information is used or disclosed for the purpose for which it was obtained or compiled or for a consistent purpose. The use or disclosure of Personal Information in any other way is in accordance with the legislation.

Retention and Disposition:

The City will retain Personal Information in accordance with the City's records retention schedules and applicable legislation. See current records retention by-law, including amendments.

Records that contain Personal Information must be securely disposed of. Disposition of information can occur by destruction or a transfer to archives (for archival records).

Security:

Personal Information must be secured for the duration of its lifecycle, including from the time it is collected to the time it is destroyed. Security measures can include administrative, technical or physical safeguards. Business units must take reasonable steps to prevent unauthorized access, unauthorized disclosure, theft, loss, misuse of Personal Information and inadvertent destruction or damage of records.

Privacy Breaches and Complaints

Privacy complaints and suspected privacy breaches must be reported to the individual's supervisor, Director – Legislative Services & City Clerk and Access & Privacy Officer immediately. If the breach or potential breach involves information technology resources, the Director – Corporate Information Technology must be notified immediately, in addition to the aforementioned.

The Director – Legislative Services & City Clerk and/or Access & Privacy Officer will make every effort to respond to the individual who reports the privacy complaint or suspected privacy breach within one business day. The situation will then be assessed by the Director – Legislative Services & City Clerk and/or Access & Privacy Officer. The Access & Privacy Officer may then proceed to investigate, work with the business unit and respond to the privacy complaint and/or breach. When required, a report will be completed on the breach and submitted to the Information and Privacy Commissioner (IPC). In addition, City staff may be required to undergo additional training or make

adjustments to work processes in order to prevent a similar breach from occurring in the future.

Roles & Responsibilities

City Manager

- Communicates this policy and promotes compliance with this policy by all City staff.

Director – Legislative Services & City Clerk

- The individual responsible for the compliance of MFIPPA, as delegated by City Council.
- Overall accountable for the protection of privacy at the City.
- Oversees the administration and decisions under MFIPPA.
- Administers the Freedom of Information processes/program.
- Provides oversight and compliance of this policy.
- Consults with business units to ensure programs comply with privacy requirements.
- Ensures Privacy Impact Assessments are completed when required by the General Manager.
- Manages privacy related incidents, complaints and breaches.
- Provides recommendations, approval of recommendations and sign-off on Privacy Impact Assessments.

Access & Privacy Officer and delegated employees

- Develops and delivers access and privacy related training.
- Develops policies and procedures with respect to access and privacy.
- Provides advice with respect to access and privacy related matters to City staff.
- Assists the public with access requests (Freedom of Information requests) and correction of Personal Information requests as required.
- Represents the City on appeals to the IPC.
- In consultation with the business unit(s) assists in drafting Privacy Impact Assessments, which includes assessing information and communicating recommendations and mitigation strategies.
- Investigates and responds to incidents, complaints and privacy breaches.

Health Information Custodian

- Monitors and enforces privacy compliance under PHIPA.
- Develops and maintains privacy policies and practices.
- Works in partnership with the Director – Legislative Services & City Clerk to identify and respond to privacy related incidents, breaches, inquiries and complaints.
- Works in partnership with the Director – Legislative Services & City Clerk to provide Privacy Impact Assessments.

Director – Corporate Information Technology and delegated employees

- Maintains technical security of hardware, networks, data, applications, software and technology systems containing, collecting, storing or processing Personal Information.
- Implements risk-based approaches to assess technology systems involving Personal Information.
- Implements privacy concepts and requirements into policies, procedures and digital infrastructure in partnership with the Director – Legislative Services & City Clerk.

Legal Services

- Provides legal research, legal advice and legal opinions, upon request, with respect to access and privacy matters.
- Represents the City on appeals to the IPC, upon request of the Director – Legislative Services & City Clerk or when deemed necessary by the City Solicitor.

Director - Human Resources & Corporate Safety

- Builds access and privacy awareness into corporate orientation and works with the Director – Legislative Services & City Clerk to improve awareness through training.

General Managers

- Implements and communicates requirements of this policy to employees under their direction.
- Ensures this policy and applicable privacy laws are followed with respect to Personal Information.
- Makes final determination as to the necessity of when Privacy Impact Assessments for projects, programs, initiatives, technologies or services are required, as requested by the Director – Legislative Service & City Clerk, as the General Manager is overall responsible for ensuring sufficient resources allow for City staff to comply with MFIPPA.

Employees (including Managers and Supervisors)

- Familiar with and complies with this policy.
- Completes mandatory access and privacy training.
- Understands responsibilities with respect to access to information and protection of privacy, including responsibilities assigned in other City policies and procedures.
- Responds to Freedom of Information requests from the City Clerk's Office, including Archives, Records and Privacy, in accordance with compliance deadlines.
- Assists the public with access to information requests, as authorized, that are of public record or part of the authorized routine disclosure.
- Works with employees involved in privacy investigations.
- Follows all records and information management practices.

REFERENCES

- *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 (MFIPPA)
- *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3, Sched. A (PHIPA)
- Information and Privacy Commissioner of Ontario

DEFINITIONS

City means The Corporation of the City of Thunder Bay.

Collection means to receive or obtain Personal Information, by any means, from or about the individual to whom the information relates.

Disclosure means the release of Personal Information, by any means.

Freedom of Information Request means a formal access to records request made under the Ontario *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA).

Personal Information is recorded information about an identifiable individual. Refer to MFIPPA subsection 2(1) for additional information. https://www.ontario.ca/laws/statute/90m56#BK1

Personal Health Information is identifying information about an individual in oral or recorded form as defined in subsection 4(1) of PHIPA. Refer to PHIPA subsection 4(1) for additional information. https://www.ontario.ca/laws/statute/04p03#BK5

Privacy Breach means an incident that involves Personal Information and/or Personal Health Information being collected, used, disclosed, retained or disposed of in a manner not consistent with provisions of applicable legislation. For example, when Personal Information and/or Personal Health Information is lost, stolen or involves unauthorized access.

Privacy Impact Assessment is a due diligence tool that analyzes the effects of projects, programs, initiatives, technologies or services on the privacy of individuals.

Information and Privacy Commissioner means the Information and Privacy Commissioner of Ontario.

Record means recorded information on any format. Refer to MFIPPA subsection 2(1) for additional information. https://www.ontario.ca/laws/statute/90m56#BK1

APPROVED BY:	City Council	***Date:***	April 8, 2024
Replacing/Amending:	10/15/96		
Originating Department:	Office of the City Clerk		
Contact:	City Clerk		
Departmental Procedural Manual:	Yes		
Affected Departments:	All		