Protection of Privacy Policy

Policy No.: No. CIMS-006
Version No.: No. 3.0
Division: City Clerk's Office
Approval date: May 26, 2022
Issued On: May 26, 2022
Subject: privacy
Keywords: accessibility, accountability, audit, breach, collection, data, divisional, documents, framework, government, information, management, MFIPPA, notice, personal, PHIPA, principles, privacy, open, operations, records, responsibility, security, transparency

Foreword

City of Toronto Information Management Policies and Standards are the official publication on the policies, standards, directives, guidelines, position papers and preferred practices given oversight under delegated authority of Toronto Municipal Code, Chapter 217, Records, Corporate (City). These publications support the City's responsibilities for coordinating standardization of Information Management in the City of Toronto.

Acknowledgements

This Policy acknowledges the efforts, subject matter expertise, and oversight provided by the following:

Project Sponsor: **Kristie Pratt** Deputy City Clerk, Corporate Information Management Services, City Clerk's Office

Divisions and Business Units:

- City Clerk's Office, Corporate Information Management Services
- Office of the Chief Information Security Officer
- People & Equity Division
- Technology Services Division

Revision History:

Version #	Version Date	Issued By	Changes in Document
1.0	July 21, 2014	City Clerk's Office	Publication of version #1
2.0	August 22, 2019	City Clerk's Office	Application Statement updated
3.0	2022	City Clerk's Office	Addition of Privacy Protection Principles (Appendix 2); updated Purpose, Principles, and Roles and Responsibilities sections

Contact Information:

Kristie Pratt
Deputy City Clerk
Corporate Information Management Services
City Clerk's Office
City Hall, 13th floor, West Tower
100 Queen Street West
Toronto ON M5H 2N2
Tel: (416) 392-9683
Kristie.Pratt@toronto.ca

Table of Contents

1.0 Introduction

Privacy plays a key role in a free, democratic society and is an essential element in maintaining public trust in government. As municipalities continue to embrace digital services, the public must feel confident that the City of Toronto protects the Personal Information in its custody or control. Privacy and access to information must be built by design into all City programs, applications, processes, projects, technology, and digital infrastructure that will collect, process, and store Personal Information.

The City of Toronto's Protection of Privacy Policy establishes guidance and principles for the responsible management of Personal Information at the City. This policy outlines privacy management accountabilities and oversight mechanisms to enable City staff to comply with the privacy requirements identified in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), other legislation may also be applicable and create obligations with respect to the protection of Personal Information or records held by the City.

The Protection of Privacy Policy is an output of the Information Management Framework, a framework developed to ensure an accountable, accessible, and trustworthy City. The Protection of Privacy Policy falls under the Framework's Open and Secure Principle which sets the requirements for privacy protection and the public service's responsibility for safeguarding Personal Information, while ensuring the delivery of services in an open and accessible manner.

2.0 Purpose

The purpose of this policy is to strengthen the City of Toronto's ability to protect Personal Information under its control or custody. This policy establishes a risk-based approach to privacy protection, sets clear accountabilities, and outlines roles and responsibilities for processes, systems, and programs that collect, use, or manage Personal Information.

This policy incorporates the principles and requirements set out in MFIPPA to ensure the City's compliance with this legislation.

MFIPPA defines **Personal Information** as recorded information about an identifiable individual. The Act clarifies that information about an identifiable individual that is collected orally on behalf of the institution is also defined as Personal Information.

To qualify as Personal Information:

- it must be about an individual in a personal capacity
- it is reasonable to expect an individual may be identified if the information is disclosed

Examples of Personal Information include:

- home address, personal email address, home telephone number, identification numbers e.g. Social Insurance Number or employee number
- correspondence between the individual and City that directly or indirectly relates to private or confidential matters. Examples of these correspondences could occur in various settings, such as through personal emails, forms, and telephone interviews
- ethnic origin, religion, age, gender, sexual orientation, marital status
- educational, medical, criminal history, employment history, or personal financial transactions
- the individual's name if it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual

Some of the above examples may not constitute Personal Information on their own; however, when combined with other information, it may constitute Personal Information (for example, a poll or survey may not contain a person's name or address, but may include information that could potentially identify an individual). The Personal Information Collection, Use and Disclosure Guideline communicates the City's responsibilities for the management of Personal Information.

Information associated with an individual in a professional, business, or official capacity is not Personal Information. MFIPPA, Section 2.1 (1) states that business identity information is not Personal Information. This includes the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity.

MFIPPA Section 2.1 (1) applies even if an individual carries out business, professional or official responsibilities from their dwelling and the contact information for the individual relates to that dwelling.

3.0 Application

This Policy applies to all City of Toronto Divisions, City employees, volunteers, and third parties engaged by the City of Toronto.

This Policy applies to all Personal Information that is under the custody or control of the City.

This policy does not apply to Personal Health Information that falls under the purview of Health Information Custodians such as Toronto Public Health, Seniors Services and Long-Term Care, and Toronto Paramedic Services as they are subject to the Personal Health Information Protection Act (PHIPA). These divisions have their own designated privacy staff. They are consulted on privacy matters that may impact Health Information Custodians.

This policy does not apply to Elected Officials, Accountability Officers, or City Agencies and Corporations.

Per the Guide to Access and Privacy for Councillors, complaints regarding non-compliance with MFIPPA will be referred by the Integrity Commissioner to the Deputy City Clerk, Corporate Information Management Services for review.

Accountability Officers
The City's Accountability Officers include the Auditor General, Integrity Commissioner, Lobbyist Registrar, and Ombudsman. The Officers report to, and are directly accountable to, City Council. The City of Toronto Act requires that the Officers independently perform their duties and establish confidentiality requirements for their information. These confidentiality requirements are recognized in Toronto Municipal Code, Chapter 3, Accountability Officers, and the City's Protection of Accountability Officers' Information Directive developed to safeguard the confidentiality of the Officers' records. In the event of a privacy breach related to any of the Accountability Officers, the City would seek the guidance of the Information and Privacy Commissioner of Ontario.

City Agencies and Corporations
Most City Agencies and Corporations are separate institutions under MFIPPA and have their own designated Head for privacy matters. The City of Toronto encourages City Agencies and Corporations to review, adopt, or update this Policy appropriate to their business circumstances.

4.0 Policy Statement

The City of Toronto will:

- Ensure all employees, volunteers, contract staff, and third parties engaged with the City share responsibility for the protection of Personal Information and comply with the provisions identified in this Policy pursuant to MFIPPA and other applicable provincial and federal legislation.

- Plan for and ensure that privacy protection requirements are embedded by design in all City programs, applications, processes, projects, technology, and technology architecture that will process Personal Information.

- Establish and communicate a set of privacy standards and guidelines to improve the protection of Personal Information by identifying, investigating, assessing, monitoring, and mitigating Personal Information privacy risks in City programs and activities involving the collection, retention, use, disclosure, and disposition of Personal Information.

- Apply this policy and related policies and practices to the collection, use, disclosure, and disposal of Personal Information.

- Clearly communicate to the public how Personal Information is collected, used, managed, disclosed, and disposed of.

- Make privacy training mandatory for all staff, volunteers, and contract staff hired by the City of Toronto and establish an employee learning plan to improve privacy awareness and best practices consistent with the complexity and sensitivity of the information they collect, have access to, and manage.

5.0 Organizational Outcomes

It is expected that by complying with this policy the City will:

- Increase trust and confidence in Toronto's municipal government.

- Ensure statutory and regulatory compliance with, and effective application of, applicable privacy legislation

- Establish rules and procedures for managing privacy breaches, investigations, audits, consultations, and other privacy matters.

- Communicate and identify roles and responsibilities for City staff, volunteers, contract staff, and parties related to the management of Personal Information.

- Integrate Privacy by Design and Access by Design principles into all new or modified architectures, technologies, programs, in order to mitigate Personal Information privacy risks in City programs and activities that involve the collection, use, disclosure, and disposition of Personal Information.

- Establish rules and procedures to strengthen data privacy by ensuring security controls for the confidentiality, integrity, and availability of information.

6.0 Principles

The City acknowledges and incorporates into this policy the ten Privacy Protection Principles which have been adopted by various jurisdictions, including the Office of the Privacy Commissioner, Canada, as guiding principles for the collection, use, and disclosure of Personal Information.

Adherence to these principles assists the City of Toronto in achieving positive outcomes by protecting and managing Personal Information. The principles are:

- Accountability
- Identifying Purposes

- Consent
- Limiting Collection
- Limiting Use, Disclosure, and Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Challenging Compliance

Refer to Appendix 2 for more details on each principle.

7.0 Roles & Responsibilities

7.1 City Manager will:

- Provide oversight and promote compliance with this Policy and Framework by all City staff.

7.2 Deputy City Managers will:

- Administer and communicate this Policy and Privacy Framework broadly to all staff within the divisions they manage.

- Champion 'Privacy by Design', by integrating protection of privacy requirements into the development, implementation, evaluation, and reporting activities of divisional programs and services within their division.

- Promote a culture and business practices that ensure City information is open by default and accessible to the greatest extent possible, while respecting security and privacy requirements of Personal Information and other confidentiality obligations.

7.3 City Clerk will:

- Approve and implement this Policy in partnership with City Divisions.

- Develop and implement policies, programs, and services for the management and protection of Personal Information in compliance with MFIPPA and other applicable codes, policies, and guidelines.

- Administer the Freedom of Information (FOI) process/program while protecting Personal Information from being released.

- Review divisional practices for the collection, use, disclosure, and authorized disposition of Personal Information.

- Consult with business areas to ensure programs meet privacy requirements as identified in this Policy, applicable legislation, privacy standards, and procedures.

- Establish privacy standards, guidelines, and procedures to support this Policy and the Privacy Framework.

- Develop training materials in collaboration with People & Equity for employee training, awareness, and skills development in Privacy and Information Management.

- Investigate complaints of information misuse and/or privacy breaches and communicate findings and recommendations (where applicable) to the complainant and Division Head.

- Produce investigation reports in response to privacy breaches and communicate recommendations and mitigation strategies to Division Heads.

- Sign-off on the Privacy Impact Assessment report for any technology, system, program, or service involving the collection or use of Personal Information or Personal Health Information.

- Authorize the disposal of Personal Information that was collected by Divisions without the appropriate authority, notice of collection statement, or other mandatory legislative requirements.

7.4 Chief Technology Officer will:

- Apply Privacy by Design and Access by Design principles in acquisition, development, design, testing, and implementation of digital infrastructure projects.

- Implement privacy concepts and requirements into policies, procedures, standards, and the Digital Infrastructure Strategic Framework.

- Ensure that project review and gating criteria involve consultation with the Chief Information Security Officer and the City Clerk for issues and exceptions relating to cybersecurity and privacy.

- Ensure that the Chief Information Security Officer and the City Clerk review and endorse decisions on cyber risk and privacy resource requirements, and that adequate funds are included in technology budgets for projects, initiatives, transformations, and acquisitions that require the processing of Personal Information.

- Review procurement documentation (such as Requests for Proposals) for technology solutions that process Personal Information and participate in the evaluation of compliance with privacy requirements when requested.

7.5 Chief Information Security Officer (OC) will:

- Define cyber security standards for technologies in conjunction with the City Clerk, Chief Technology Officer, and relevant business divisions that ensure adequate safeguards and compliance for those technologies or technological processes that collect, use, disclose, or retain Personal Information including services, technologies, or systems managed by third-party vendors or agents on behalf of the City.

- Define cyber security requirements such as those outlined in the Corporate Cyber Security Policy, to ensure City of Toronto information and data, applications, systems, and networks, particularly those collecting, storing, or processing Personal Information, are secure, reliable, and trusted.

- Implement a risk-based approach to assess all technology systems involving the collection or use of Personal Information. Where applicable, security risk assessments as per the Corporate Cyber Security Policy will be conducted.

7.6 Chief People Officer, People & Equity will:

- Provide the educational platforms and learning management tools necessary to facilitate privacy awareness and compliance training, as well as host training materials provided by the City Clerk's Office.

- Include privacy management training as part of the performance management process.

- Work with the City Clerk's Office, in consultation with Technology Services Division and Office of the Chief Information Security Officer, to build privacy awareness content, annual privacy training refresher for all staff, and training into all new staff orientation programs.

- Provide the City Clerk's Office with insights into privacy awareness and compliance training, including analytics on participant engagement and evaluation of training programs.

7.7 Division Heads will:

- Implement this Policy and the Protection of Privacy Framework and communicate requirements to staff under their direction.

- Ensure compliance with this Policy and that Personal Information is collected, used, disclosed, and disposed of in accordance with legislation and associated regulations, standards, and other City policies.

- Incorporate privacy protection concepts and principles into divisional strategies and plans.

- Restrict access to Personal Information to those individuals who require it in order to perform their duties and where access is necessary for the administration of their business.

- Inform staff of the legal and administrative consequences of any inappropriate or unauthorized access to, or collection, use, disclosure, or disposition of Personal Information related to a particular program or activity.

- Consult with the City Clerk, Chief Technology Officer, and the Chief Information Security Officer during the planning stages, before any procurement, and prior to the implementation of any technology, system, program, or service involving the collection, use, disclosure, or disposition of Personal Information.

- In collaboration with the City Clerk, City Manager, Chief Technology Officer, Chief Information Security Officer, and Chief Purchasing Officer, require that vendors, contractors, or anyone acting as an agent on behalf of the City comply with this Policy and that the privacy rules, concerns, and requirements are embedded in all documents governing the service provision, procurement, or relationship between the City and the aforementioned.

- Require that staff, vendors, contractors, and agents maintain a level of privacy awareness appropriate with their responsibilities through agreements, training, policy, and supporting reference materials.

- Receive formal privacy investigation reports from City Clerk's Office and make final decisions about the handling of a complaint.

- Be accountable for privacy risk treatment and acceptance within their respective divisions.

- Understand the repercussions for accepting high or critical privacy risks including prosecution, fines, and/or reputational damage.

- Report back to the City Clerk and Chief Information Security Officer on privacy risk mitigation/treatment actions outlined in privacy and security assessments conducted by the OC on their projects and initiatives.

7.8 All Employees, Third Parties (including Vendors and Contractors) and Volunteers will:

- Comply with MFIPPA and other applicable legislation that governs the collection, use, disclosure, and disposition of Personal Information under their control.

- Complete mandatory privacy awareness and training for the appropriate handling of Personal Information to understand their responsibilities to protect privacy in executing their operational duties.

- Review the privacy resources and educational materials (e.g. guidelines, fact sheets) available in the City's Protecting Privacy at Work webpage.

- Manage Personal Information that is part of a business record in accordance with the City's Responsible Record Keeping Directive, Information Management Accountability Policy, and the requirements identified in this Policy.

- Review and understand their responsibilities when developing any information collection tool that may be used to collect personal or confidential information.

- Follow specific procedures and use the approved Law Enforcement Request form for disclosing Personal Information to a law enforcement agency in Canada.

- Review and understand the privacy responsibilities noted in various city policies such as:
    - City's Acceptable Use of Information Technology Assets Policy
    - City's Video Surveillance Policy
    - City's Digital Infrastructure Plan
    - Privacy Impact Assessment Policy

- Cooperate with CIMS' Privacy Staff or anyone else appointed to investigate privacy breaches or non-compliance with legislation.

8.0 References

- City of Toronto (2017). Code of conduct Complaint Protocol for Members of Council. Retrieved from: https://www.toronto.ca/wp-content/uploads/2017/10/96bf-code-of-conduct-complaint-protocol-for-members-of-council.pdf
- City of Toronto, City Clerk's Office (2018). Information Management Accountability Policy. Retrieved from: https://www.toronto.ca/wp-content/uploads/2018/07/8ec6-information-management-accountability-policy.pdf
- City of Toronto, City Clerk's Office (2013). Privacy Impact Assessment Policy. Retrieved from: https://www.toronto.ca/wp-content/uploads/2017/08/8f83-PIA-

Policy.pdf City of Toronto, City Clerk's Office. Protecting Privacy at Work web page. Retrieved from: http://insideto.toronto.ca/clerks/cims/privacy-resources.htm

- City of Toronto, City Clerk's Office (2019). Protecting Privacy in City Surveys. Retrieved from: http://insideto.toronto.ca/clerks/policies/files/privacy-city-surveys.pdf
- City of Toronto, City Clerk's Office (2012). Responsible Record-Keeping Directive. Retrieved from: https://www.toronto.ca/wp-content/uploads/2017/08/9741-Responsible-Record-Keeping-Directive-Final_1.pdf
- City of Toronto, City Clerk's Office (2006). Security Video Surveillance Policy. Retrieved from: https://www.toronto.ca/legdocs/2006/agendas/council/cc060725/admcl021a.pdf
- City of Toronto, City Clerk's Office (2020). Understanding Notice of Collection Statements Guideline. Retrieved from: http://insideto.toronto.ca/clerks/policies/files/collection-statements.pdf
- City of Toronto, City Clerk's Office. Law Enforcement Request for Personal Information form. Retrieved from: https://www.toronto.ca/wp-content/uploads/2018/02/8eca-Law-Enforcement-Request-for-Personal-Information.pdf
- City of Toronto, City Clerk's Office (2015). Law Enforcement Request for Personal Information Procedures - What to do When a Police Officer Asks for Information. Retrieved from: https://www.toronto.ca/wp-content/uploads/2018/02/8748-What-to-do-When-a-Police-Officer-Asks-for-Information.pdf
- City of Toronto, City Clerk's Office (2005). Managing a Privacy Breach Guideline. Retrieved from: http://insideto.toronto.ca/clerks/policies/files/managing-privacy-breach.pdf
- City of Toronto, Office of the Chief Information Security Officer (2021). Cyber Security Policy. Retrieved from: http://insideto.toronto.ca/ciso/files/cyber-security-policy.pdf
- City of Toronto, Technology Services Division (2018). Acceptable Use Policy. Retrieved from: http://insideto.toronto.ca/itweb/policy/pdf/acceptable_use.pdf
- City of Toronto, Technology Services Division (2022). Digital Infrastructure Strategic Framework. Retrieved from: https://www.toronto.ca/city-government/accountability-operations-customer-service/long-term-vision-plans-and-strategies/smart-cityto/digital-infrastructure-strategic-framework/
- Information and Privacy Commissioner of Ontario (2010). Access by Design: The Seven Foundational Principles. Retrieved from: https://www.ipc.on.ca/wp-content/uploads/2010/05/accessbydesign_7fundamentalprinciples.pdf
- Information and Privacy Commissioner of Ontario (2011). Privacy by Design: The Seven Foundational Principles. Retrieved from: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

- Office of the Privacy Commissioner of Canada (2019). PIPEDA Fair Information Principles. Retrieved from: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

9.0 Policy Approval

Provided by Kristie Pratt, Deputy City Clerk, Corporate Information Management Services, City Clerk's Office, May 26, 2022.

10.0 Policy Review

The City Clerk's Office will review this Policy and its effectiveness at the three-year mark from the effective date of this Policy, or earlier if warranted.

Appendix 1: Protection of Privacy Framework

Protection of Privacy Framework
The City of Toronto protects personal privacy to support public confidence in municipal government. This framework should be used as a tool to help users understand privacy requirements in the City of Toronto.

PRIVACY BY DESIGN	Privacy requirements are built into city programs, processes, projects, and technology architecture, ensuring privacy protection is proactive and embedded in design.
IMPLEMENTATION	City Staff access and apply privacy policies and practices in the collection, use, disclosure, and secure disposal of Personal Information.
ACCOUNTABILITY	City staff must ensure Personal Information is protected.
TRANSPARENCY	Individuals are confident that their Personal Information is responsibly used and consistent with the purpose for which it was collected.
TRAINING AND AWARENESS	City staff roles and responsibilities in protecting Personal Information are clearly communicated through awareness and training.

Examples of how the Framework is used day-to-day include:

- **Privacy by Design**: Privacy requirements are included in new technology projects that process Personal Information and are built into system design and architecture.
- **Transparency**: Individuals are advised on all City forms how their Personal Information will be used, and are provided a City contact to answer concerns about the collection.
- **Implementation**: The daily application of formal privacy practices and processes as required by MFIPPA, PHIPA, and other privacy legislation to foster a culture of accountability and trust.
- **Training and Awareness**: Mandatory privacy training, commensurate with job responsibilities, for all City staff whose progress is monitored and reported annually by Division Heads.

Appendix 2: Privacy Protection Principles

Ten Privacy Protection Principles have been adopted by various jurisdictions, including the Office of the Privacy Commissioner, Canada as guiding principles for the collection, use, and disclosure of Personal Information. The Protection of Privacy Policy supports implementation of these principles.

Principle 1 - Accountability

The City of Toronto is legally responsible for Personal Information under its custody and control. In the City of Toronto, the City Clerk is the designated head of the Institution under MFIPPA and is accountable for ensuring processes and policies are in place for the management of Personal Information. The Protection of Privacy Policy and the Information Management Accountability Policy are two policies that outline staff responsibilities for managing Personal Information.

The City of Toronto is accountable for the Personal Information it collects, uses, discloses, and retains. The City of Toronto ensures accountability by:

- implementing procedures to protect Personal Information
- establishing procedures to receive and respond to complaints and inquiries
- training staff and communicating to staff information about the organization's policies and practices, and
- developing information to explain the organization's policies and procedures

Principle 2 - Identifying Purposes

MFIPPA outlines the circumstances in which the City must provide notice to an individual when collecting their Personal Information and circumstances where no notice is required.

Notice of Collection Statements and other privacy requirements are outlined in MFIPPA, Part II, Protection of Individual Privacy. Corporate Information Management Services' Information Collection Unit can assist Divisions and staff understand their obligation to provide notice, and apply privacy principles to information collection tools.

Principle 3 – Consent

Under MFIPPA, the City's ability to collect Personal Information from an individual is based on having legal authority, not simply upon obtaining the individual's consent. Nonetheless, consent does play a role in MFIPPA's privacy protections.

Institutions governed by MFIPPA can only collect Personal Information directly from the individual to whom the information relates, unless the collection is covered under one of the provisions of section 29 of the Act.

An individual may provide consent for an indirect collection of their Personal Information or for a secondary use of Personal Information if such use was not identified at the time of collection or is not for a consistent purpose. An institution can only disclose Personal Information where the individual provides consent, or if such disclosure is in accordance with Section 32 of the Act.

Consent for indirect collection or secondary use as described above should be in writing, and the specific information for which consent is given must be identified.

Principle 4 - Limiting Collection

Collection of Personal Information must be limited to the minimum amount needed for the purposes identified by the collecting organization. Any new information collection initiative or technology where Personal Information is collected shall include only those data elements that are necessary for the initiative.

Principle 5 - Limiting Use, Disclosure, and Retention

Unless the individual consents otherwise or it is required by law, Personal Information can only be used or disclosed for the purposes for which it was collected, or for a consistent purpose. A consistent purpose is defined as the use of that information, only if the individual might reasonably have expected such use, and it is reasonably compatible with the purpose for which it was obtained or compiled.

Personal information should not be kept in the City's repositories for longer than required under legislation. Municipal Code Chapter 217 sets out the retention schedules for various types of records. CIMS' Records Services Unit supports compliance with this principle by working with Divisions to develop approved Records Series Classifications, and Retention and Disposition schedules.

Disclosure of Personal Information is subject to the provisions of MFIPPA. Personal Information cannot be disclosed except to the individual to whom the information relates, or their authorized representative.

Personal Information that has been de-identified using anonymization standards can be released and published as Open Data. Anonymization is a process whereby the primary identifier in a dataset is replaced or redacted and a string of characters used in its place. The risk of re-identification is usually very low if best practices for anonymization are followed. However, where a dataset or subset is small, and there are other linked elements of personally identifiable information, the risk for re-identification increases.

All City Division Heads are responsible for ensuring that employees receive appropriate training on their roles and responsibilities in protecting Personal Information.

Principle 6 - Accuracy

Personal Information must be as accurate, complete, and as up to date as possible in order to properly satisfy the purposes for which it is to be used. Personal Information that is used on an ongoing basis, including information that is disclosed to third parties, should also be accurate and up to date, unless limits to the requirement for accuracy are clearly set out. Data collectors may use various techniques to ascertain accuracy and data quality, such as repeating questions, or asking questions in a different format.

Principle 7 – Safeguards

The City must protect Personal Information with security safeguards that are appropriate for the level of sensitivity of the information and the format and medium of storage.

As the City continues to embrace digital services, Technology Services Division will rely on risk assessments by the Office of the Chief Information Security Officer to identify risks and recommend necessary safeguards and protection. Safeguarding Personal Information in the digital realm requires activities such as:

- conducting a Privacy Impact Assessment (PIA) to determine risks and provide recommendations for systems that will collect and store data.
- determining where data is collected, stored, and managed by third parties. Adequate security safeguards will be developed by the Technology Services Division and vetted by the Office of the Chief Information Security Officer. These may include encryption standards as well as network security controls. A thorough risk assessment process and additional safeguards must be put in place through contract language.

Principle 8 – Openness

This principle promotes transparency about Personal Information in the City's custody and control and supports adoption of policies and best practices regarding its collection, use, disclosure, retention, and disposition.

The City demonstrates its commitment to openness in many ways, including application of Notice of Collection Statements that communicate the legal authority for the collection and the principal purpose, or purposes, for which the Personal Information can be used. Staff are prohibited from using Personal Information for purposes not identified in the Notice of Collection. In turn, City staff are made available to answer questions about the collection process.

The City of Toronto also makes detailed information about its policies and practices relating to the management of Personal Information publicly and readily available. Divisions must be open about their policies and practices with respect to the management of Personal Information. Individuals shall also be able to obtain information about an organization's policies and practices without unreasonable effort, in a form that is generally understandable.

Principle 9 - Individual Access

This principle outlines that individuals have a right to access the Personal Information that an organization holds about them. They also have the right to challenge the accuracy and completeness of the information and have that information amended as appropriate.

Upon request, an individual must be informed of the existence, use, and disclosure of their Personal Information and be given access to that information. The Access Unit of the City Clerk's Office has a formal Freedom of Information (FOI) process to provide access to information held by the City. Individuals may request their information through the formal FOI process.

Principle 10 - Challenging Compliance

An individual shall be able to challenge an organization’s compliance with MFIPPA and with the other privacy protection principles. Any challenge should be addressed to the City Clerk, City of Toronto, or addressed to the Information and Privacy Commissioner, Ontario. An individual has the right to appeal a decision that the City makes with respect to the collection or disclosure of Personal Information about them.

Appendix 3: Definitions

Term	Definition
Access by Design	The fundamental principles that encourage public institutions to take a proactive approach to releasing information, making the disclosure of government-held information an automatic process where possible.
Collection	To gather, acquire, receive, or obtain Personal Information from or about the individual to whom the information relates, by any means and from any source.
Disclosure	To release or make available Personal Information by any method (e.g., sharing information by any means such as orally, sending an email, posting online) to anybody or person.
Disposition	The action taken with regards to Personal Information including destruction, transfer to another entity, or permanent preservation.
Form	A structured template or tool, irrespective of the media in which it appears, used to capture, compile, transmit, communicate, and record specific business information that causes an action to occur. The term “form” applies equally to paper forms and digital information collection tools
Information Management	The means, by which the City of Toronto responsibly plans, creates, capture, organizes, protects, uses, controls, shares, disposes of, and evaluates its information, and through which it ensures that the value of that information is identified, trusted, and used to the fullest extent.
Personal Information	Personal Information is recorded information about an identifiable individual. Refer to MFIPPA, Section 2 (1) for additional information. http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m56_e.htm
Personal Health Information	Personal Health Information is identifying information about an individual that relates to their health or providing health care to the individual. Refer to PHIPA, Section 4 for additional information: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm#BK5
Privacy	A set of interests and rights that an individual has regarding his/her ability to control the collection, use, disclosure, and retention of his/her own personal information that is in the custody or control of a third party (i.e. City of Toronto). Privacy is a limited, not an absolute right in all situations. Personal information may be collected from or

	about an individual, used, disclosed, or retained without their consent of individuals where specific legislation permits.
Privacy Breach	The improper or unauthorized creation, collection, use, disclosure, management, retention, or disposition of Personal Information.
Privacy by Design	To build privacy and data protection into the design specifications and architecture of information and communication systems and technologies from the earliest planning stages, in order to facilitate compliance with privacy and data protection principles. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
Privacy Impact Assessment (PIA)	PIA is a due diligence exercise to analyze the effects of a technology, system, program, or service design on the privacy of individuals. The City of Toronto develops and maintains privacy impact assessments for all new or modified programs and activities that involve the use of Personal Information or Personal Health Information for an administrative or operational purpose.
Privacy Risk	The likelihood that individuals will experience direct or indirect harms as a result of inadequate or failed internal processes and systems, staff error, and/or external events.
Retention Period	The length of time records should be maintained in a certain location or format for administrative, legal, fiscal, historical, or other purposes.
Risk Management Plan	A report that identifies how a project sponsor will accept, avoid, or reduce the privacy risks identified for a technology, system, program, or service.
Third Party	An individual or entity that is involved in City business but is not a principal party or employee of the City of Toronto. This may include consultants, vendors, and service providers. Third parties are required to comply with the restrictions and conditions that are necessary to enable the City to comply with all these requirements.
Threat Risk Assessment (TRA)	The TRA is the process for identifying the threats to confidentiality, integrity, or availability of Information Technology (IT) assets, assessing current risks for each IT assets based on existing or proposed controls, analysing, and quantifying the risk levels for the vulnerable IT assets, and providing recommendations to lower the risks to an acceptable level.
Use	The purpose(s) for which the information was obtained or compiled.
Vulnerability Assessment (VA)	The VA is the process for identifying potential system level or technical weaknesses in the Information Technology (IT) system that could be exploited to compromise the confidentiality, integrity, and availability of IT assets, analysing, and quantifying the risk levels for each vulnerability identified, and providing recommendations to mitigate the risks to an acceptable level.