

Information Collection Policy

Policy No.: No. CIMS-016

Version No.: 1.0

Division: City Clerk's Office

Approval date: April 25, 2025

Issued On: May 1, 2025

Subject: privacy, information management

Keywords: information collection, protection of privacy



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:

- Corporate Information Management Services Division
 - Corporate Information and Strategy & Policy
 - Privacy & Information Collection
 - Records Services
 - Archival Services
 - Access
- Technology Services Division
- Office of the Chief Information Security Officer
- Legal Services

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

Contact Information:.....	2
1. Introduction	4
2. Purpose	4
3. Authority	4
4. Application.....	5
5. Scope	5
6. Principles.....	7
7. Policy Statement	7
8. Personal Information Collection Requirements	9
9. Roles & Responsibilities.....	13
City Manager will:	13
Deputy City Managers will:	13
City Clerk will:	13
City Clerk's Office's Corporate Information Management Services (CIMS) Unit will:	14
Chief Technology Officer will:	15
Chief Information Security Officer will:	15
Legal Services will:	16
Division Heads will:	16
All Staff will:	17
10. Policy Approval.....	18
11. Policy Review	18
Appendix A: Definitions.....	18
Appendix B: Policy and Legislation References.....	20
Appendix C – Privacy Protection Principles	21

1. Introduction

The City defines information collection as gathering, acquiring, receiving, or obtaining any information from or about the individual to whom the information relates, by any means and from any source. It is a key government process that enables the City to deliver services, foster civic engagement, assess program performance, allocate resources, and support employee success.

Government efforts towards digital transformation and business modernization have introduced services, programs, and technology tools that make it easier for the City to collect information from and about its employees and the people who live, work, and access services in Toronto. Electronic forms and cloud infrastructure make it efficient to collect, share, and integrate data. The City leverages smart hardware such as sensors and internet of things devices to passively collect information. Increasingly, technology-enabled information collection tools have the capability to inconspicuously and autonomously generate their own data and insights from user interactions, in contrast to traditional paper-based forms and surveys, which are intended to simply record information provided by an individual.

The Information Collection Policy supports business processes, infrastructure, and strategies that allow the City to meet its legislative obligations to protect privacy, build public trust, and protect information against unauthorized access and use throughout its lifecycle. This Policy establishes the roles and responsibilities for enabling services, programs, and technology tools used to collect information, and the legislative requirements for City Divisions to collect Personal Information, specifically.

2. Purpose

This Policy identifies the requirements and stakeholder commitments needed to ensure that information collection practices fulfill requirements identified in the [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#), the City of Toronto's [Protection of Privacy Policy](#), and the City of Toronto's [Data for Equity Strategy](#).

This Policy formalizes the role of the City Clerk's Office's Corporate Information Management Service (CIMS) in providing City Divisions with consultative services to assess, develop, and implement services, programs, and technology tools that collect information.

3. Authority

This Policy is issued in order to satisfy the City's compliance obligations under the [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#).

Under the [Toronto Municipal Code, Chapter 169](#), the City Clerk shall set objectives for the management of information in the City and is delegated the powers and duties of the Head of Privacy set out in the [Municipal Freedom of Information and Protection of](#)

[Privacy Act \(MFIPPA\)](#). These duties and powers give the City Clerk authority to ensure reasonable measures are in place to protect Personal Information in the City's custody or control.

This Policy must be read in conjunction with other City policies, standards, and strategies, including, but not limited to:

- [Protection of Privacy Policy](#)
- [Information Management Accountability Policy](#)
- [Privacy Impact Assessment Policy](#)
- [Information and Data Governance Policy](#)
- [Digital Image Management Policy](#)
- [Information Protection Classification Standard](#)
- [Data for Equity Strategy](#)

4. Application

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

The Policy does not apply to the City's Elected Officials, Agencies and Corporations, or its Accountability Offices, including the Auditor General, Integrity Commissioner, Lobbyist Registrar, and Ombudsman. The City encourages these groups to review, adopt, or update this Policy as appropriate to their business needs.

5. Scope

This Policy addresses all circumstances under which the City collects information from or about an individual, including programs, services, technology systems, and information collection tools. Information collection tools include, but are not limited to, forms, surveys, sign-up sheets, paper and electronic applications, complaints submissions, paper and electronic questionnaires, email subscriptions, permits, sensors, smart hardware, internet of things devices, photographs, audio and video recordings, social media applications, and interviews. Information collection tools can also include cookies and user monitoring software tools that track online activity and capture system-generated metadata that can identify individuals, such as IP Addresses and location logs.

This Policy addresses different kinds of identifying information prescribed in applicable legislation. This includes Personal Information, Business Identity Information, and Socio-Demographic Information (as defined below).

Personal Information

[MFIPPA](#) defines Personal Information as recorded information about an identifiable individual, and lists several types of information that are specifically included in the

definition. The Act specifies 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 reasonable to expect an individual may be identified if the information is disclosed.

Please review the City's [Protection of Privacy Policy](#) and [Section 2 \(1\) of MFIPPA](#) for the fulsome definition of Personal Information.

Some identifiers outlined in MFIPPA may not constitute Personal Information on their own, but when integrated or aggregated, may constitute Personal Information. For example, a poll or survey may not collect a person's name or address but may collect information that could indirectly identify an individual.

Business Identity Information

As provided for MFIPPA, Business Identity Information (BII) is recorded information about an individual provided in a business, professional, or official capacity, including the name, title, contact information or designation that identifies a person in a business, professional, or official capacity. This includes business information gathered from City of Toronto employees, volunteers, and contractors by the City, and information provided to the City by an individual about their business. This information is specifically excluded from the definition of Personal Information.

Socio-Demographic Information

Socio-Demographic Information (SDI) is recorded information that describes personal characteristics and social identities, such as age, language, race, First Nations, Inuit, Métis identity, Canadian-born or immigrant citizenship status, disability, gender, sexual orientation, income, and place of residence.

Socio-demographic information does not necessarily constitute Personal Information if it is de-identified, analyzed, and/or presented in a way that does not allow an individual to be identified. It can be collected in ways that limit the ability to identify an individual or may be aggregated from individual responses for service and program development, evaluation, and improvement.

Exclusions

Personal Health Information

This Policy does not apply to the collection of Personal Health Information governed by the Personal Health Information Protection Act. The City's Health Information Custodians must address additional considerations when planning for and collecting Personal Health Information.

Employment Information

As stated in [MFIPPA Section 52 \(3\)](#) this Policy does not apply to employment information that is excluded under MFIPPA. This exclusion applies to records collected, prepared, maintained, or used by or on behalf of the City in relation to any of the following:

- Proceedings or anticipated proceedings before a court, tribunal, or other entity relating to labour relations or the employment of a person by the City.
- Negotiations or anticipated negotiations relating to labour relations or the employment of a person by the City between the City and a person, bargaining agent, or party to a proceeding or an anticipated proceeding.
- Meetings, consultations, discussion, or communications about labour relations or employment-related matters in which the City has an interest.

6. Principles

This Policy adopts the Privacy Protection Principles established by the City's [Protection of Privacy Policy](#):

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

The principles are reproduced in [Appendix C](#) for reference.

7. Policy Statement

The City commits to:

- Confirming legal authority to collect Personal Information for a given purpose prior to initiating collection.
- Limiting collection, use, and disclosure of Personal Information to only what is necessary for administrative and operational service delivery, and what is required by law.
- Only using Personal Information in accordance with [Section 31 of MFIPPA](#).
- Providing Notice of Collection Statements for the collection of Personal Information in accessible formats that comply with the [Accessibility for Ontarians with Disabilities Act](#) and the [Ontario Human Rights Code](#).

- Collecting Personal Information directly from the individual to whom the information relates, unless another manner of collection has been authorized by that individual, or the collection is required by law.
- Ensuring individuals can access their Personal Information collected and maintained by the City of Toronto.
- Allowing individuals to update, correct, or withdraw their Personal Information in accordance with applicable legislation.
- Where required, obtaining express consent prior to the collection of Personal Information.
- Where required, obtaining express consent prior to changing how Personal Information is used and/or disclosed.
- Clearly explaining what Personal Information the City collects and the purposes for which it is used or shared with others in a way that is easy for City staff, residents, businesses, and visitors to understand.
- Adhering to the [Data for Equity Strategy](#).
- Embedding equity, inclusion, and reconciliation principles into the design and delivery of services, programs, technology systems, and information collection tools used to collect Personal Information, Business Identity Information, and Socio-Demographic Information.
- Using the Equity Lens Tool to identify impacts of programs, services, technology systems, and information collection tools for equity-deserving communities.
- Integrating the [City-Recommended Survey Questions](#) into services, programs, technology systems, and information collection tools that collect Personal Information, Business Identity Information, and Socio-Demographic Information.
- Adopting the City's [Core and Optional Socio-demographic Data Elements](#) when designing program, services, technology systems, and information collection tools that collect Personal Information, Business Identity Information, and Socio-Demographic Information.
- Applying City-mandated security measures by-design to the services, programs, technology systems, and information collection tools that collect Personal Information, Business Identity Information, and Socio-Demographic Information to protect City information from unauthorized access, disclosure, and destruction.
- Designing services, programs, technology systems, and information collection tools that collect Personal Information, Business Identity Information, and Socio-Demographic Information that adhere to the City's [Corporate Identity Guidelines](#).
- Delivering services, programs, technology systems, and information collection tools that collect Personal Information, Business Identity Information, and Socio-Demographic Information in compliance with the [Accessibility for Ontarians with Disabilities Act \(AODA\)](#).

Corporate Information Management Services commits to:

- Establishing an Information Collection Policy in alignment with MFIPPA, the Protection of Privacy Policy, the Information Management Accountability Policy, the Information and Data Governance Policy, and the Data for Equity Strategy.
- Supporting the development of services, programs, technology systems, and information collection tools across City Divisions to collect only the Personal Information necessary for administrative and operational service requirements.
- Monitoring the evolution and lifecycle of divisional programs, services, technology systems, information collection tools and policies that support information collection.
- Centralizing and standardizing information about services, programs, technology systems, and information collection tools to support appropriate, transparent, and purposeful information collection, sharing, and use.
- Completing [Information Management Assessments](#) (IMAs) and [Privacy Impact Assessments](#) (PIAs) for services, programs, technology systems, and information collection tools that collect Personal Information.

8. Personal Information Collection Requirements

The requirements in this section reflect the privacy protection measures MFIPPA prescribes for the collection of Personal Information.

Prior to initiating collection of Personal Information, City Divisions must integrate and satisfy this Policy's requirements in their programs, services, technology systems, and information collection tools. City Divisions must ensure that any third parties collecting Personal Information on behalf of the City comply with this Policy's requirements.

City Divisions are encouraged to apply these requirements to the collection of Business Identity Information and Socio-Demographic Information that does not contain Personal Information.

Application of these requirements to Business Identity Information and Socio-Demographic Information is not required by MFIPPA, or mandatory for City Divisions. However, applying these requirements to programs, services, and information collection tools that collect BII and SDI promotes privacy by design and:

- protects the City in case of unintentional collection of Personal Information. Public-facing, web-based information collection tools that are intended to be used by businesses or City contractors (such as user account portals, web forms, and service request submission tools) present a residual risk that members of the public may access them and submit their Personal Information. Smart hardware and IoT devices used to monitor City assets, and cameras installed in City facilities, may also unintentionally collect Personal Information.

- reduces risks arising from integration of Socio-Demographic Information and/or Business Identity Information, which may result in identification or re-identification of Personal Information.
- protects the privacy of individuals who work from home or manage business operations from their residences, and for whom a breach of their Business Identity Information may result in some of the same real harms as a breach of Personal Information.
- builds trust between City Divisions and staff when collecting Business Identity Information from employees. Identifying the purposes for which Business Identity Information is collected from employees, how it is collected, how it will be used, and who employees can direct questions about the information collection process to, promotes transparency and accountability. It is especially important to consider information collection requirements when collecting Business Identity Information through smart hardware or employee monitoring tools.

Authorization

The City Division must not collect Personal Information unless the collection is:

- Authorized by a Council directive, a municipal bylaw, or a legal statute, such as provincial legislation, or federal legislation.
- Used for the purpose of law enforcement.
- Necessary to the proper administration of a lawfully authorized activity.

If a bylaw or legislation does not specifically refer to information collection, the Division must reference the specific section of an act or bylaw which authorizes the activity or program for which the information must be collected.

Prior to initiating collection, authorization must be obtained from the individual to whom the information relates. Unless collection is otherwise authorized by [MFIPPA, section 29](#), City Divisions must obtain authorization in the form of express consent from the individual to whom the information relates. When authorization for collection is provided orally, the City Division collecting Personal Information must create a written record of:

- The name of the individual providing consent;
- The information to which the consent relates; and
- How the individual was notified about the purposes of the collection, use, and/or disclosure of the information.

Parents, guardians, and/or Powers of Attorney may authorize the collection of Personal Information from and about individuals without decision-making capacity, including children under the age of 16 years old.

The City Division collecting the Personal Information must get authorization in the form of express consent of the individual from whom the information relates prior to changing how Personal Information is used, shared, or disclosed.

Individuals must be given the option to refuse or withdraw authorization for the collection and use of their Personal Information at any time.

Minimization

The City Division collecting Personal Information must de-identify and aggregate Personal Information wherever possible.

The City Division collecting Personal Information must classify, retain, and disposition Personal Information according to, [Toronto Municipal Code Chapter 217, Records, Corporate \(City\) Schedule A – Records Retention Schedule](#).

City Divisions must not collect, use, or disclose Personal Information if other information that does not identify an individual will serve the purpose of the collection, use, or disclosure.

City Divisions must review the features, functions, and parameters of technology systems and information collection tools and enable only those that collect Personal Information that is relevant to, and necessary for, business and service delivery. Any features or functions that are not compatible with the legal authority and purposes for collection must be disabled.

Necessity

Collection of Personal Information must be limited to what is required for administrative and operational service delivery, and what is required by law.

The City Division collecting PI must be able to demonstrate that the information is rationally connected and necessary to the operating program or activity to which it relates.

The City Division collecting PI must be able to demonstrate that the information is likely to be effective in meeting the objectives of the program or activity to which it relates.

The City Division collecting PI must be able to demonstrate that there are no other less privacy-invasive ways to effectively achieve the objectives of the program or activity to which the PI relates.

The City Division collecting PI must be able to demonstrate that the loss of privacy is proportional to the objectives of the program or activity to which the PI relates.

City Divisions must not collect, use, or disclose more Personal Information than is reasonably necessary to meet the purpose of the collection, use, or disclosure to which the PI relates.

Notice of Collection

The City Division collecting Personal Information must communicate information about the legal authority, purpose, and use in a Notice of Collection Statement to individuals. Notice of Collection Statements are written in plain language and presented in accessible formats and must include:

- A citation of the legal authority that authorizes collection of Personal Information.
- The specific purpose for collecting Personal Information, including if the Personal Information will be used for secondary purposes or disclosed to any other Divisions or third parties.
- The title, business address, and phone number of a person employed by the City who can answer questions about the collection.

Notice of Collection Statements may be provided in writing – on an application form, on a posted sign, or in any other manner which informs the individual about the collection, or orally – such as over the phone or in person.

Any secondary use, sharing, or disclosure of Personal Information must be clearly documented in the Notice of Collection Statement. Secondary use includes integration of Personal Information from multiple datasets and sharing or disclosure of Personal Information within a City Division.

Notice of Collection Statements must be developed prior to initiating collection of Personal Information.

The City Division collecting Personal Information must make Notice of Collection Statements available to individuals at the point of information collection. For example, embedding the statement in an application form if collecting information directly from an individual, or placing signage with Notice of Collection details in public places where information is collected from a sensor or camera.

Manner of Collection

Personal Information must be collected directly from the individual to whom the information relates, unless the individual has authorized indirect collection, or indirect collection is permitted under [MFIPPA sec.29](#), or other applicable legislation.

Circumstances that permit indirect collection of Personal Information under MFIPPA include:

- Where other statutes provide authority to collect in another manner.
- Where institutions have legal authority to disclose Personal Information.
- For conducting a proceeding or a possible proceeding before a court or tribunal.
- For law enforcement purposes.
- For determining suitability of an honour or award.

Accessibility

Notice of Collection statements must be written in plain language English.

Notice of Collection statements must take individual needs into account when a uniform statement is inappropriate to ensure that there are no barriers to access and comprehension. It is not always reasonable to believe that a written notice will sufficiently inform an individual of the purposes of a collection, use or disclosure. For example, when low literacy skills, a language barrier, or a vision disability prevent an individual from understanding a written or printed notice, the City Division collecting the information must find another way to communicate relevant details about the purpose, use, and disclosure of the information being collected.

9. Roles & Responsibilities

City Manager will:

- Promote compliance with the Information Collection Policy by all City staff.

Deputy City Managers will:

- Administer and ensure communication of this Policy to all staff within their cluster.
- Ensure divisional programs and services within their cluster integrate the information collection requirements identified in this Policy.
- Promote a culture and business practices that ensure City information is shared and accessible to the greatest extent possible, while respecting privacy and security requirements.

City Clerk will:

- Approve and implement this Policy in collaboration with corporate partners.
- Develop and offer corporate programs and services to the City that promote responsible information collection and privacy practices.
- Develop and implement programs and services for the management and protection of Personal Information, Business Identity Information, and Socio-Demographic Information in compliance with MFIPPA and other applicable legislation, policies, and standards.
- Designate Corporate Information Management Services (CIMS) to manage the Information Collection Program and other programs that work with and evaluate

technologies collecting information, to promote good information collection practices.

- Individually, or jointly with the Chief Technology Officer and Division Heads, review PIA Reports and documented risks prior to implementation of any program, service, technology system or information collection tool involving the collection or use of Personal Information.
- Consult with the Division Head, Chief Technology Officer, Chief Information Security Officer, and City Manager regarding any programs, services, technology systems, or information collection tools that pose significant privacy risks corporately.

City Clerk's Office's Corporate Information Management Services (CIMS) Unit will:

- Establish privacy standards, guidelines, and procedures to support this Policy, the [Protection of Privacy Policy](#), and the [Privacy Impact Assessment Policy](#).
- Provide Divisions consultative corporate services to embed privacy by design into their project, programs, services, and information collection tools.
- Develop training materials in collaboration with the People & Equity Division for employee training, awareness, and skills development in privacy and information collection.
- Determine if a service, program, technology system, or information collection tool requires an [Information Management Assessment](#) and/or [Privacy Impact Assessment](#).
- Complete assessments, such as Information Management Assessments and Privacy Impact Assessments for projects, programs, services, and information collection tools.
- Establish a governance approach to address concerns and provide corporate direction on information collection.
- Establish and promote best practices for information collection, and the proper management of this information once collected, including privacy protections, access to information, records retention classification, and appropriate disposition.
- Provide consultation and training to City Divisions on the development of programs, services, technology systems, and information collection tools that collect Personal Information.
- Maintain and make available paper and electronic form templates used to collect Personal Information.
- Assist Divisions through consultations with the Information Collection Unit to obtain privacy recommendations that encourage compliance with legislation, corporate policies, standards, and best practices.
- Administer a forms inventory tool for finding and accessing authoritative, approved City information collection tools.

Chief Technology Officer will:

- Develop and implement architecture and technology standards applicable to records, data, and information management.
- Apply Privacy by Design principles in the acquisition, development, design, testing, and implementation of technology systems, including information collection tools that collect Personal Information.
- Implement technology systems, including information collection tools that collect Personal Information in coordination with City Divisions.
- Ensure that the Chief Information Security Officer and the City Clerk are consulted about 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.
- Maintain a catalogue of corporately available technology systems, including information collection tools that can be used for collection of Personal Information.

Chief Information Security Officer will:

- Conduct Threat Risk Assessments for technology systems, including information collection tools.
- Provide Risk Treatment Plans to Divisions to identify cybersecurity risks and outline measures to mitigate risks.

Chief People Officer will:

- Support Divisions and create conditions, supports, and resources to drive alignment with the Data for Equity Strategy and Guidelines to inform why, when, and how to collect, manage, use, analyze and report on Socio-Demographic Information in a consistent and equitable manner.
- Provide the educational platforms and learning management tools necessary to facilitate privacy and information collection awareness and compliance training, as well as host training materials provided by the City Clerk's Office.
- Collaborate with the City Clerk's Office and other corporate partners to develop, implement and monitor corporate strategies, policies, standards, and procedures in the areas of equity and data in relation to information collection.
- Provide advisory supports to Divisions in leveraging disaggregated data and embedding equity into work for evidence-based and accountable decision-making that is responsive to the needs of all Torontonians, particularly First Nation, Inuit and Metis (FNIM), Black, and other equity-deserving groups.
- Work with the City Clerk's Office, Technology Services Division, and Office of the Chief Information Security Officer, to build privacy and information collection awareness and training for all staff, including into all new staff orientation programs.

Legal Services will:

- Assist with development of Notice of Collection Statement components related to legal authority and/or purpose.
- Review terms of use agreements, privacy statements, and memoranda of understanding.
- Consult with CIMS on privacy and/or information management recommendations upon request.
- Provide guidance on compliance with applicable legislation and risk management options.

Division Heads will:

- Ensure compliance with this Policy and that Personal Information is collected in accordance with legislation and associated regulations, standards, and other City policies.
- Be accountable for developing Notice of Collection Statements for each program, service, technology system, or information collection tool used to collect Personal Information.
- Ensure the legal authority for collection of Personal Information is accurate and valid prior to initiating collection of Personal Information.
- 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 program, service, technology system, or information collection tool used to collect Personal Information.
- Completed the required CIMS assessments of their new technology systems.
- Ensure Personal Information is used only for the purposes set out in the Notice of Collection Statement.
- Obtain the consent of the individual to whom Personal Information pertains prior to using it in a manner that is inconsistent with the initial purpose for which it was collected.
- Collect only the Personal Information required to meet business and operational needs.
- When indirectly collecting Personal Information, maintain a record with the date and details of the authority for indirect collection, including the Personal Information to be collected, source of the Personal Information, and name of the collector/information about the information collection tool.
- Manage, report, and contain any potential or confirmed privacy breach in accordance with the City's [Privacy Breach Protocol](#).
- Ensure that governance to support information collection is incorporated into Divisional roles and processes to support sustainment and information quality.

- Provide funding and resources for development and implementation of services, programs, technology systems, and information collection tools that collect Personal Information.
- Make programs, services, technology systems, and information collection tools that collect Personal Information accessible, in compliance with the [Accessibility for Ontarians with Disabilities Act](#).
- Design information collection tools in compliance with the City's [Corporate Identity Policy](#), [Common Data Elements for City Forms Standard](#), and [City Recommended Survey Question Bank](#).
- Be accountable for accepting and/or mitigating information management, privacy, and security risks identified in services, programs, technology systems, and information collection tools that collect Personal Information, prior to initiating collection.
- Maintain the currency of services, programs, technology systems, and information collection tools that collect Personal Information.
- 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.

All Staff will:

- Foster a culture of openness and transparency through the use of approved information collection tools.
- Adhere to the Information Collection Policy and its applicable standards and guidelines.
- Protect privacy and ensure accessibility when collecting, using, processing, and sharing Personal Information.
- Ensure accessible options are available for consent for the collection of Personal Information.
- Conduct themselves in a manner that allows the City to 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 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](#), [Protection of Privacy Policy](#), and the requirements identified in this Policy.

- Review and understand their responsibilities when developing programs, services, technology systems, and information collection tools that may be used to collect Personal Information.
- 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](#)
 - [Law Enforcement Request for Personal Information Procedures](#)
 - [City's Digital Infrastructure Strategic Framework](#)
 - [Privacy Impact Assessment Policy](#)
 - [Digital Image Management Policy](#)

10. Policy Approval

Provided by Kristie Pratt, Deputy City Clerk, Corporate Information Management Services, City Clerk's Office, April 25, 2025.

11. Policy Review

The City Clerk's Office will review this Policy and its effectiveness as warranted.

Appendix A: Definitions

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.

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 City data, information, and records, 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.

Forms Inventory Tool 3.0: A web-based City repository for information collection consultation submissions, reviews, inquiries, and supporting correspondence, which

ensure compliance with legislation, corporate policies, standards, and best practices. It is designed to support City Divisions collecting information through all phases of the consultation lifecycle.

Information collection: To gather, acquire, receive, or obtain information from or about the individual to whom the information relates, by any means and from any source.

Information collection tools: The methods and infrastructure used to gather information about individuals. They may include paper forms and surveys, digital forms and surveys, interviews, public consultations, email registrations, signup sheets, registration forms, photography and videography, email, biometric devices, web applications, mobile applications, and internet of things devices.

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.

Information Management Assessment: A structured review process that ensures City Divisions incorporate information management (IM) into the design and implementation of technology projects and initiatives. Conducted by CIMS, they ensure all domains of IM are embedded from project conception through implementation to achieve a state of readiness to manage information.

Internet of things device: A physical object that has been programmed to connect to the internet and exchange data with other devices and systems.

Personal Information: Personal Information that is recorded information about an identifiable individual. Refer to MFIPPA, Section 2 (1) for a fulsome definition of Personal 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.

Privacy impact assessment: 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.

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.

Appendix B: Policy and Legislation References

- [Municipal Code Chapter 217, Records, Corporate \(City\)](#)
- [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#)
- [Information Management Accountability Policy](#)
- [Information and Data Governance Policy](#)
- [Protection of Privacy Policy](#)
- [Privacy Impact Assessment Policy](#)
- [Digital Image Management Policy](#)
- [Information Protection Classification Standard](#)
- [Common Data Elements for City Forms Standard](#)
- [Data for Equity Strategy](#)
- [Responsible Record-Keeping Directive](#)
- [Managing a Privacy Breach Guideline](#)
- [City Clerk's Office: Information Management Framework \(IMF\)](#)
- [Privacy Impact Assessment Form](#)
- [Information Management Assessment Form](#)
- [Information Management Assessment Fact Sheet](#)
- [Understanding Notice of Collection Statements Guideline](#)
- [Acceptable Use Policy](#)
- [Corporate Identity Policy](#)
- [City of Toronto's Vision Statement on Access, Equity, and Diversity](#)

Appendix C – 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](#), [Information Management Accountability Policy](#), and [Information and Data Governance Policy](#) 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 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 exemptions in 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 must 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, must 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 public 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.