

Information Management Accountability Policy

Policy No.: No. CIMS-003

Version No.: No. 3.0

Approval date: March 10, 2023

Division: City Clerk's Office

Issued On: April 20, 2023

Subject: Information Management

Keywords: Information management, data, accessibility, principles, accountability, transparency, records, documents, digital information, framework, recordkeeping

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
- Legal 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 2012	City Clerk's Office	Publication of version #1
2.0	June 2018	City Clerk's Office	Publication of version #2
3.0	April 2023	City Clerk's Office	Updates to Roles & Responsibilities, Application, Compliance, and alignment to relevant policies.

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. Introduction	4
2. Application.....	4
3. Policy Statement	5
4. Principles.....	5
5. Roles & Responsibilities	6
5.1 City Manager will:	6
5.2 Deputy City Manager(s) will:	6
5.3 City Clerk will:	6
5.4 Chief Information Security Officer will:	7
5.5 Chief Technology Officer will:	7
5.6 Health Information Custodians will:.....	8
5.7 Chief People Officer, People & Equity will:	8
5.8 Division Heads will:.....	8
5.9 All Employees will:	9
6. Compliance	10
7. References.....	10
8. Policy Approval.....	11
9. Authority	11
10. Policy Review	11
Appendix	12
Appendix A: Definitions.....	12

1. Introduction

Information collected, created and used by the City of Toronto is a corporate resource. Information that is accurate, useable and accessible supports open, transparent and accountable local government, and improves customer service and program delivery.

The public expects access to City information and the protection of their privacy. City leadership and management expect information to be current, correct and managed responsibly throughout the information lifecycle. City information encompasses records in all formats—paper, electronic, digital images, physical storage media, and structured data collected and stored in systems.

The City's [Information Management Framework \(IMF\)](#) provides the foundation upon which Information Management (IM) policies, standards, procedures, and guidelines are built. The IMF's goals are to manage information as a corporate resource, which can be made available to the public through all stages of its use, design a government that makes information accessible and open while protecting privacy, and improve customer service and civic engagement. The City is committed to having policies and practices that ensure transparency in the management of City information and to making information available to the public.

The Information Management Accountability Policy is an output of the IMF and supports the development of Information Management policies, practices, standards and directives for accountability and openness.

With the implementation of this policy, the City will:

- Integrate Information Management practices into service delivery;
- Integrate Information Management practices into business planning;
- Invest in greater Information Management awareness, training and communication to improve a culture of collaboration and information sharing;
- Support Information Management, privacy and access in modernized work environments;
- Support the City's efforts to manage information in all formats; and
- Ensure alignment between this Policy and other corporate frameworks for information, information technology, and digital infrastructure planning efforts.

2. Application

This Policy applies to all City of Toronto Divisions, City employees, volunteers and contract employees hired 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 (HICs), such as Toronto Public Health (TPH), Seniors Services and Long-Term Care (SSLTC), and Toronto Paramedic Services (TPS) 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 HICs.

This policy does not apply to Elected Officials, Accountability Officers or City Agencies and Corporations. The City of Toronto encourages City Agencies and Corporations to review, adopt or update this policy appropriate to their business circumstances.

3. Policy Statement

The City of Toronto commits to:

- A culture of collaboration and information-sharing;
- The management of information as a corporate resource through its lifecycle;
- The long-term preservation of City records, regardless of format, which warrant acquisition by the City of Toronto Archives;
- Ensuring access to information is open by default;
- Building in access to information and protection of privacy by design into technology and processes;
- The duty to document decisions and the decision-making process;
- The protection of personal and confidential information;
- Ensuring the safe handling and storage of information while working remotely (see the [Information Management Remote Work Guideline](#));
- Enabling technology to improve the management of information;
- Employee training on records, Information Management, and privacy commensurate with their job duties; and
- Compliance with this Policy and other legislative and policy obligations.

4. Principles

- The Information Management Accountability Policy is the foundational policy within the City's Information Management policy structure;
- Information is a valuable corporate resource which must be organized, managed, and accessible to drive efficiency, support transparency and accountability, and improve public services;
- Information is managed to improve openness and transparency, ensuring trust in local government;
- Documenting City decisions and services contributes to legislative compliance and good customer service. Employees have a [Duty to Document](#) complete and accurate business activities and decisions, regardless of the communication methods and tools used;
- Information shall be open and accessible by default and design to the fullest extent permitted by law and subject to legislative obligations to protect privacy and confidentiality;
- All employees share responsibility for the protection of personal information privacy (see the [Protection of Privacy Policy](#));

- The continuous and effective management of information is included in established governance structures, mechanisms and resources;
- All employees share responsibility for the proper management of records and information, ensuring the authenticity, reliability, and usability of information and providing timely access to records and information; and
- The City will provide employees with the tools and resources required to comply with the roles and responsibilities identified in this Policy.

5. Roles & Responsibilities

5.1 City Manager will:

- Promote openness, access and collaboration throughout the organization;
- Promote the management of information through its lifecycle, from records creation or receipt to classification, maintenance, disposition, and destruction; and
- Exercise all the responsibilities and duties of the "head" for the purposes of the [Municipal Freedom of Information and Protection of Privacy Act, 1990 \(MFIPPA\)](#), as an alternate for the City Clerk, when the City Clerk is unable to do so as delegated under [Toronto Municipal Code Chapter 169, City Officials](#).

5.2 Deputy City Manager(s) will:

- Ensure Information Management requirements are integrated into the development, implementation, evaluation, and reporting of technologies, programs, and services within their service group;
- Ensure that each Division under their purview develops and integrates Information Management considerations, requirements and goals into their Divisional business and strategic planning;
- Ensure information is shared and accessible to the greatest extent possible and in a timely manner, while complying with legislative privacy requirements; and
- Ensure projects and initiatives in their Divisions include Information Management, privacy, and access by design.

5.3 City Clerk will:

- Lead the corporate development and implementation of strategies, policies, standards, procedures, best practices, programs, and systems as a framework to promote City transparency, accountability, and the management of and access to City information;
- Exercise all the responsibilities and duties of the "head" for the purposes of [MFIPPA](#), as delegated to the City Clerk in the [Toronto Municipal Code Chapter 169, City Officials](#);
- Provide Divisions consultative corporate services to embed effective and efficient legislatively-required lifecycle management of records and information by design into their operations, services, technology and digital infrastructure projects;

- Exercise the authority to establish or amend the [City's Records Retention Schedule](#) in accordance with the requirements of the [Toronto Municipal Code Chapter 217, Corporate Records](#);
- Ensure the separation, segregation, and protection of information belonging to Accountability Officers and Elected Officials where required;
- Preserve and provide access to the City's archival records regardless of media and format;
- Develop and implement preservation policies, standards, procedures and strategies to ensure information with long-term retentions remain useable throughout the records lifecycle;
- Collaborate with corporate partners to lead and promote corporate records and Information Management training and awareness; and
- Provide records and Information Management oversight and guidance in business processes.

5.4 Chief Information Security Officer will:

- Provide leadership and vision for cybersecurity policy and initiatives for the City;
- Proactively work with management and City Divisions to implement and enforce practices on standards for cybersecurity;
- Understand and articulate the impact of cybersecurity on digital and physical assets as well as business operations through privacy, penetration testing and threat risk assessments;
- Have oversight over cyber assessment and privacy advisory services, ensuring the achievement of City business outcomes where business processes are dependent on technology; and
- Collaborate with senior leadership, all levels of management, and Corporate and Divisional partners to determine acceptable level of risks for the City by translating and implementing risk mitigation approaches and/or solutions to mitigate the City's security risk exposure.

5.5 Chief Technology Officer will:

- Integrate information and records management, privacy and access requirements by design into technology architectures, policies, standards and implementation activities, in accordance with the requirements of [Municipal Code Chapter 217, Corporate Records](#) and [MFIPPA](#), in both operational and capital projects;
- Provide strategic direction for information technology, digital infrastructure, and electronic government service delivery;
- Develop and maintain related technology policies, standards, procedures and architectures; and
- Implement and support the City's [Open Data Policy](#), including managing an inventory of information.

5.6 Health Information Custodians will:

- Be accountable for the Information Management practices affecting Personal Health Information in their Divisions, as a Health Information Custodian as identified in the [Personal Health Information Protection Act, 2004 \(PHIPA\)](#); and
- Be accountable for the Information Management practices affecting information in their Division.

5.7 Chief People Officer, People & Equity will:

- Collaborate with the City Clerk to develop a culture of collaboration and information sharing through the delivery of Information Management training and awareness programs; and
- Build records, Information Management, and privacy education and awareness training and skills development courses into all new employee orientation programs to facilitate a culture change.

5.8 Division Heads will:

- Promote openness, access and transparency through collaboration and information-sharing across the Division and with the public;
- Manage records and information in their Division in accordance with [MFIPPA](#), [Chapter 217 of the Toronto Municipal Code](#), the [Protection of Privacy Policy](#), the [Digital Image Management Policy](#), the [Responsible Record Keeping Directive](#) and other relevant legislation and City policies;
- Make information available in response to [Freedom of Information \(FOI\)](#) requests, in accordance with legislated timeframes;
- Consult with the [City Clerk's Office, CIMS](#), before undertaking technology and digital infrastructure projects to embed effective and efficient legislatively required lifecycle management of records and information;
- Restrict access to personal information, in accordance with the appropriate [information protection classification categories](#), to those individuals who require access to personal information in order to perform their duties and where access is necessary for the lawful administration of their business;
- Manage records in compliance with the City's [Records Retention By-laws](#), [Responsible Recordkeeping Directive](#), and other relevant City policies and legislation;
- Communicate, implement, and support compliance with all records and Information Management policies and standards established by the City Clerk in their Divisions;
- Designate Divisional staff to represent the Division, as appropriate, on corporate initiatives that impact how they collect, manage, store, publish, provide access to, and use City information;
- Ensure strategic planning occurs for Information Management goals, targets, and outcomes in the Division, with accountabilities and monitoring practices outlined;

- Ensure the Divisions maintain an updated [Routine Disclosure Plan](#), which is communicated to staff, and made accessible to the public;
- Document decisions and decision-making processes, regardless of the communication method used (e.g., meetings, instant messaging, email, voice messaging, etc.);
- Ensure staff are aware of their responsibilities to document decisions and apply proper record keeping rules to service delivery and projects;
- Ensure vendors comply with all applicable records, information management, privacy, and access policies and legislation;
- Ensure the communication methods used to conduct City business or deliver City programs and services, such as instant messaging, are in accordance with the [City of Toronto Act](#), City's [Acceptable Use Policy](#) (for City of Toronto staff only), [Protection of Privacy Policy](#), [Remote Work Guideline](#) and other relevant legislation, policies, and standards;
- Manage information in the Division in accordance with the City's [Acceptable Use Policy](#); and
- Maintain the authenticity, reliability, usability, and integrity of records and information in order to meet projects, delivery of services, operational needs, and accountabilities.

5.9 All Employees will:

- Be aware of and fulfill the requirements of good recordkeeping practices and the [responsibility to document decisions](#);
- Inform themselves through records, Information Management, and privacy education and awareness, training, and skills development courses;
- Comply with records, Information Management, information security, confidentiality, and privacy protection policies, standards, and practices;
- Manage information in such a way that it provides concise, accurate, and complete evidence of their decisions, transactions, and activities, regardless of the communication methods (e.g., meetings, instant messaging, email, voice messaging, etc.) and ensure that information is stored in the appropriate repository;
- Collect, use, manage, disclose, and dispose of personal information that is part of a City record in accordance with [MFIPPA](#), [PHIPA](#), [Chapter 217 of the Toronto Municipal Code](#), the City's [Protection of Privacy Policy](#), [Remote Work Guideline](#), and other relevant legislation and associated regulations, standards, and City policies;
- Foster a culture of openness and transparency through collaboration and lawful information-sharing across Divisions; and
- Manage information securely when using collaboration tools with internal and external parties.

6. Compliance

Failure to comply with this Policy may result in disciplinary action up to and including dismissal.

This policy directs the City to be compliant with [MFIPPA](#), [Chapter 217 of the Toronto Municipal Code](#), the [City of Toronto Act](#), and other laws applicable to Information Management and privacy accountabilities by:

- Requiring institutions subject to MFIPPA, Chapter 217 of the Toronto Municipal Code, the City of Toronto Act, and other applicable laws to develop, document, and implement measures to manage their records and information.

Individuals who wilfully disclose personal information in contravention of MFIPPA, or individuals who alter, conceal, or destroy a record, or cause any other person to do so, with the intention of denying a right under MFIPPA to access the record or information contained in the record, is guilty of an offence and liable to a fine not exceeding \$5,000.

7. References

- [Acceptable Use Policy](#)
- [City of Toronto Act](#)
- [Digital Image Management Policy](#)
- [Digital Infrastructure Strategic Framework](#)
- [Information Protection Classification Framework](#)
- [Information Protection Classification Standard](#)
- [Information Management Framework](#)
- [Information Management Policies and Procedures](#)
- [Municipal Freedom of Information and Protection of Privacy Act, 1990](#)
- [Open Data Policy](#)
- [Personal Health Information Protection Act, 2004](#)
- [Privacy Impact Assessment Policy](#)
- [Protection of Privacy Policy](#)
- [Records Metadata Standard](#)
- [Responsible Recordkeeping Directive](#)
- [Routine Disclosure Plans](#)
- [Toronto Municipal Code, Chapter 169, Officials, City](#)
- [Toronto Municipal Code, Chapter 217, Records, Corporate \(City\)](#)
- [Working Remotely - Information Management & Privacy Guideline](#)

8. Policy Approval

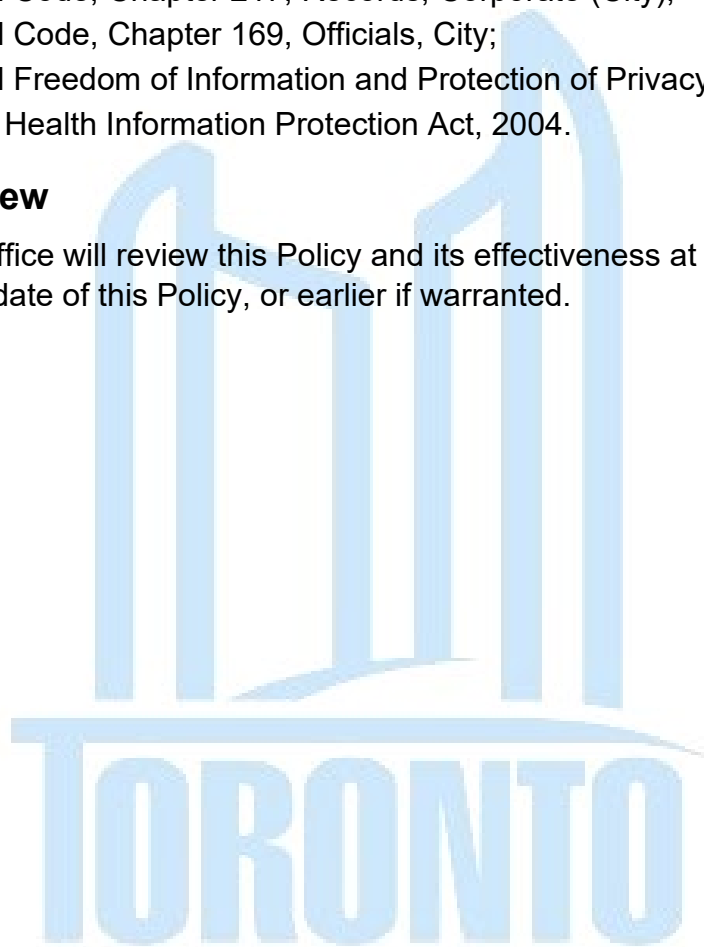
Provided by Kristie Pratt, Deputy City Clerk, Corporate Information Management Services, City Clerk's Office
March 10, 2023

9. Authority

1. City of Toronto Act, 2006;
2. Municipal Code, Chapter 217, Records, Corporate (City);
3. Municipal Code, Chapter 169, Officials, City;
4. Municipal Freedom of Information and Protection of Privacy Act, 1990; and
5. Personal Health Information Protection Act, 2004.

10. 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

Appendix A: Definitions

Confidential Information – Information in the possession of, or received in confidence by the City that the City is either prohibited from disclosing, or is required to refuse to disclose, under the Municipal Freedom of Information and Protection of Privacy Act, or other legislation. Includes, but is not limited to, privileged information, draft by-laws or staff reports, third party information, personal information, technical, financial or scientific information and any other information collected, obtained or derived for or from City records that must or may be kept confidential under the [Municipal Freedom of Information and Protection of Privacy Act](#), the [Personal Health Information Protection Act](#), or the [City of Toronto Act](#).

Digital Infrastructure – All technology assets that create, exchange or use data or information in a digital form as a part of their operation, as well as all data collected or used by the aforementioned technology assets.

Freedom of Information Request – Formal requests for records of the City of Toronto. FOI requests should not be submitted for information that is already available on the City website, from a City division by request, or for information that is held by other governments or government agencies.

Information Management – The means, by which the City of Toronto responsibly plans, creates, captures, organizes, protects, uses, controls, shares, disposes, and evaluates its information (including records, data, and digital images), and through which it ensures that the value of that information is identified and used to the fullest extent.

Personal Health Information – Identifying information about an individual in oral or recorded form, if the information is both: 1. in the custody or control of a City Staff member, who as a result, or in connection, of this Staff member performing their workplace responsibilities to the City in relation to any of the following tasks: {(a)acting as a health care practitioner; a health service provider; placement co-ordinator; medical officer of health; or, (b)operating in whole or in part, a hospital; psychiatric facility; independent health facility/community health facility; community health/mental health centre, program, or service; long-term care home; care home; home for special care; retirement home; pharmacy; laboratory/specimen collection centre; or ambulance service}; and; 2. the information: (a) relates to the individual's physical, or mental health; providing health care to the individual; health care payments; health care eligibility; eligibility for health care coverage; (including the identity of the individual's health care provider; the identity of the individual's substitute decision-maker; health history of the individual's family; and health number); or, (b) is a plan setting out the home and community care services a health service provider would provide to the individual.

Personal Information – Recorded information about an identifiable individual, such as (but not limited to): address, race, religion, gender, family status, employment history, medical history, blood type, DNA, any identifying number assigned to the individual, personal opinions or views of an individual about another individual, correspondence of a personal or confidential nature from an individual. For more information, refer to the personal information interpretation under [MFIPPA](#), S.2

Record – Information, however recorded or stored, whether in printed form, on film, by electronic means or otherwise, and includes documents, financial statements, minutes, accounts, correspondence, memoranda, plans, maps, drawings, photographs and films – [City of Toronto Act, 2006](#), s.3 (1).

Routine Disclosure – A process to enhance transparency by providing access to information without going through a formal Freedom of Information request.

