

Information and Data Governance Policy

Policy No.: CIMS-016

Version No.: 1.0

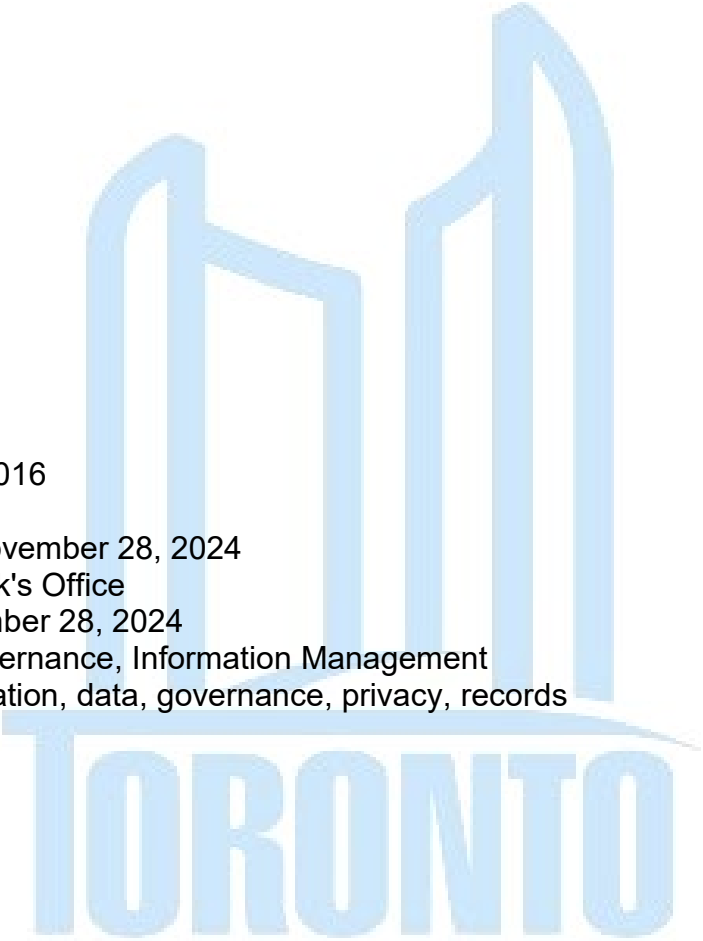
Approval date: November 28, 2024

Division: City Clerk's Office

Issued On: November 28, 2024

Subject: Data Governance, Information Management

Keywords: information, data, governance, privacy, records

The logo for the City of Toronto, featuring a stylized blue outline of the city's skyline above the word "TORONTO" in a bold, blue, sans-serif font.

TORONTO

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:

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

Divisions and Business Units:

- City Manager's Office
- Financial Services
- Office of the Chief Information Security Officer
- People & Equity
- Technology Services Division

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. Scope	5
3. Information and Data Governance Competencies	5
4. Application	7
5. Principles	7
6. Information and Data Governance Roles.....	9
7. Roles & Responsibilities	10
7.1 City Clerk will:	10
7.2 Chief Information Security Officer will:	11
7.3 Chief Technology Officer will:	11
7.4 Chief People Officer, People & Equity will:	12
7.5 Division Heads will:	13
7.6 All Employees will:	14
8. Compliance.....	16
9. References	16
10. Policy Approval.....	18
11. Authority	18
12. Policy Review	18
Appendix A: Definitions.....	19



1. Introduction

Information and data—including metadata—collected, created, and used by the City of Toronto are corporate resources of the organization. Data is the raw material used to represent information, or from which information can be derived, and can be represented as text, numbers, graphics, images, sound, or video. Information is data that has been given value through assessment, interpretation, or compilation in a meaningful form.

Information and data governance (IDG) is defined as the exercise of authority, control, and shared decision-making (accountability, planning, monitoring, and enforcement) over the management of information and data, to ensure authenticity, integrity, and usability of information and data throughout their lifecycles, according to legislation, policies, and best practices. Information governance is driven by legal, business, and compliance requirements, while aligning with strategic and operational goals and objectives. Data governance is often seen as a subset of information governance, focusing on the integrity, storage, and lifecycle management of structured data assets. Effective data governance is a key component of information governance.

The City's [Information and Data Governance Framework \(IDGF\)](#) provides the foundation upon which information and data governance policies, standards, procedures, and guidelines are built. The vision of the IDGF is for City information and data to be optimized and used to their fullest potential to improve City programs and the lives of the people who live, work, and access services in Toronto, while being collected and managed in an open, safe, secure, purposeful, and consensual manner that builds public trust and does not do harm.

The Information and Data Governance (IDG) Policy is an output of the IDGF and supports the management, protection, and use of City information and data within the City. Information and data play a critical role in informing decision-making, enhancing service delivery, and ensuring transparency, integrity, and accountability. This Policy allows for information and data to be treated as valuable City assets while working in the bounds of information management, data governance, privacy, security, equity and accessibility requirements and legislation.

This Policy is informed by and aligns with the following provincial and municipal legislation:

1. The [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#), with reference to the City's operations generally.
2. The [Personal Health Information Protection Act \(PHIPA\)](#), with reference to specific City operations which constitute Health Information Custodians (HICs), as defined by PHIPA.
3. The [City of Toronto Act, 2006 \(COTA\)](#), with reference to specific record retention and security requirements for all City information.

4. [Toronto Municipal Code, Chapter 217, Records, Corporate \(City\)](#), with reference to managing information and records and specific record retention requirements.

This Policy is aligned with the provisions of these pieces of legislation, as well as the City's [Information Management Framework](#), [Information Management Accountability Policy](#), [Protection of Privacy Policy](#), [Digital Infrastructure Strategic Framework \(DISF\)](#), [Data for Equity Strategy](#), and other related Information Management, data governance, and data collection legislation, strategies, frameworks, and policies.

In addition, this Policy aligns with industry standards and best practices, such as those outlined in the [DAMA Data Management Body of Knowledge \(DAMA-DMBoK\)](#), [International Standards Organization \(ISO\) 38505 – IT – Governance of Data](#), and [ISO 24143:2022 – Information and documentation – Information Governance – Concept and principles](#).

2. Scope

This Policy applies to all electronic City information, data, and records—including metadata—created, received, processed, transmitted, stored, reported, and procured during City business, administration, or delivery of City services, and the governance of that information and data. Data, when given necessary context and structure, can be captured under the definition of "Record" in the City of Toronto Act, MFIPPA, and the Toronto Municipal Code, Chapter 217, and such data must be retained in accordance with the applicable retention and other requirements. For the purposes of this policy, the following key concepts are defined as follows:

- **Data** is the raw material used to represent information, or from which information and records can be derived, represented as text, numbers, graphics, images, sound, or video.
- **Information** is data that has been given value through assessment, interpretation, or compilation in a meaningful form.
- **Records** are all documented information, regardless of media format, that provide verifiable evidence of an organization's functions.
- **Metadata** is data describing context, content and structure of records and their management through time, and it can describe the properties of a document or file.

3. Information and Data Governance Competencies

The Policy fosters a common vision of information and data-related practices, promotes consistent, efficient, and coordinated responses to information and data governance issues, and enhances communication and collaboration across City programs, technologies, and staff.

Effective information and data governance requires an extensive, active, and iterative approach that covers many aspects of information and data governance, management, and stewardship. This section introduces that landscape at the City, and the competencies and goals that support it. Each of these areas of competency requires training and change management activities supported by increased information and data literacy for the City to achieve and deliver them.

Policy Development: Research, forecasting, development, reviews, and collaboration on information and data governance policy artifacts including, but not limited to, strategic plans, frameworks, directives, policies, standards, guidelines, procedures, and fact sheets. Policies will define organizational roles and responsibilities in the governance of information and data, codify legislative requirements and best practices that affect information and data governance, and respond to evolving challenges, trends, and technology shifts with a policy response.

Communication: Clear, simple, and regular communication on information and data governance strategies, frameworks, policies, tools, and services within the City. This includes improving and providing proactive communication, awareness, and promotion of policy artifacts, objectives, and training.

Master Data and Metadata: Standardizing master data, reference data, and other corporate data entities, attributes, and relationships across the organization to enhance data interoperability, findability, and improve data quality.

Data Quality: Formalizing the detection and recording of data quality issues, assessments, proactive and reactive treatment and resolution methods, and other data quality enhancements.

Data Architecture and Infrastructure: Designing and building integrated data infrastructure and the capacity to support enterprise data management, data analytics, data interoperability, and business intelligence.

Information and Data Lifecycle Management: Lifecycle management of information and data as business assets from their creation, capture, or procurement, through their organization and version control, storage, use, publication, control, and protection to their disposition, throughout which the value of the information and data as a business asset can be leveraged.

Information and Data Protection, Access, Sharing, and Collaboration: Governance of the exchange of, access to, and sharing of information and data within the City, or with external partners and the public, including considerations on sharing restrictions, risk tolerance, and facilitation of information and data protection and legal holds.

Cyber Security: The practice of protecting business applications, data, and supporting infrastructure from digital attacks, theft, or damage. This involves a range of measures

including technologies, processes, and practices designed to safeguard information and ensure the integrity, confidentiality, and availability of data and services.

Data Analytics & Business Intelligence: Improving data analysis and visualization capabilities to assist in decision-making. This includes the deployment and administration of corporate data analytics and business intelligence tools.

4. Application

This Policy applies to all City of Toronto Divisions, City employees, volunteers, third-party vendors, and contract employees, including sub-contractors, hired by the City of Toronto. Corporate partners referenced in this Policy refer to corporate offices responsible for providing a broad range of programs and services to support Divisions. This includes the City Clerk's Office, the City Manager's Office, Technology Services Division, and Office of the Chief Information Security Officer.

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 adapt this Policy appropriate to their business circumstances.

5. Principles

The City commits to adhering to the following principles outlined in this Policy, drawn from the City's [Information & Data Governance Framework](#). In doing so, the City aims to enhance the trustworthiness of its information and data resources, promote informed decision-making, and ensure accountability and transparency.

Equity and inclusion objectives and criteria are integrated into each of the Framework's principles. People working with City information and data must consider how to translate the City's [Vision Statement on Access, Equity & Diversity](#) for projects and programs involving information and data. This includes:

- Maximizing the collective benefit of information and data for Indigenous, Black, and equity deserving groups.
- Respecting the information and data sovereignty of First Nations, Inuit, and Metis (FNIM) Nations, including Constitutional and Treaty rights.
- Recognizing the authority of Indigenous, Black, and equity-deserving groups to control and access their information and data.

- Working to ensure the voices, experiences, and perspectives of FNIM, Black, and equity-deserving groups are sought and reflected in the development of information and data policies and processes.
- Using inclusive and accessible language, methods, and tools when collecting information and data.
- Using and analyzing information and data in culturally appropriate ways, evaluating the methodologies and approaches used to collect and store information data, and their effect on its neutrality.

Information & Data Governance Framework Principles:

- **Findable:** City information and data are findable in a straightforward way that facilitates appropriate use by both people and computers.
- **Accessible:** City information and data are retrieved and accessed by an authorized person for an authorized purpose. The City provides procedures, standards, and tools for accessing data assets, including data protected by legislation, including but not limited to the [Municipal Freedom of Information and Protection of Privacy Act](#), [Personal Health Information Protection Act](#), [Toronto Municipal Code Chapter 217, Records, Accessibility for Ontarians with Disabilities Act](#), and the [Child, Youth and Family Services Act](#).
- **Interoperable:** City information and data are created and managed in common formats and standards to ensure appropriate access and use across tools and systems, and to facilitate collaboration and data sharing. The City designs technology and data architecture in an anticipatory manner that considers and builds protection of privacy and interoperability across systems and data streams by design.
- **Reusable:** City information and data are used and reused, with appropriate consent and control, to its fullest potential.
- **Ethical:** Information and data collection, use, storage, and disclosure are responsive and inclusive to the needs of all people who live, work, and access services in Toronto, including FNIM, Black, and equity-deserving groups, and employee Communities of Inclusion. Information and data collection and use strives to build trust and relationships with FNIM, Black, and equity-deserving communities and employee Communities of Inclusion.
- **Safe and Secure:** The City has comprehensive security measures and systems in place, that ensure authorized access to and appropriate use of City information and data.
- **Trusted and Open:** City information and data are managed in a way that promotes trust and accountability. The City ensures information and data are accurate, understandable, complete, and fit for its intended use.

6. Information and Data Governance Roles

Effective implementation of information and data governance is supported by the adoption of common roles assigned to each City data asset. This section describes key roles that form the backbone of the City's information and data governance structure, in order to maintain information and data integrity, reliability, and accountability.

Role	Description
Data Owner	<p>Individuals who are accountable for data assets within specific data domains with the ability to make and enforce decisions related to the data regardless of who collects or who manages it.</p> <p>The Data Owner is accountable for the implementation of policies and guidelines that define the appropriate use of the data, ensuring that appropriate steps are taken to protect data, and ensuring compliance with relevant legislative requirements for retention and disposition. They are responsible for appointing Data Stewards and Data Custodians, as appropriate.</p>
Data Stewards	<p>Individuals who understand the business processes and the data being produced within those processes. Data Stewards can represent the data assets on behalf of the Data Owners. Data stewards are often categorized as executive data stewards, business data stewards, or coordinating data stewards based on their day-to-day responsibilities.</p> <p>Data stewards are responsible for:</p> <ol style="list-style-type: none"> 1. The identification of operational and business intelligence data requirements within an assigned subject area 2. The quality of data names, business definitions, data integrity rules, and domain values within an assigned subject area 3. Compliance with regulatory requirements and conformance to internal data policies and data standards 4. Application of appropriate security controls 5. Analyzing and improving data quality 6. Identifying and resolving data related issues.

Data Custodian	<p>Individuals who understand the technological and system architecture requirements to support data management activities defined by the Data Stewards.</p> <p>Data Custodians are responsible for the safe custody, transport, and storage of the data, and implementation of business rules. They may work within the Division but can also be corporate partners, vendors, or contractors.</p>
----------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7. Roles & Responsibilities

7.1 City Clerk will:

- 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](#);
- Direct the corporate development and implementation of strategies, policies, standards, procedures, and best practices for the governance and management of, access to, and protection of City information and data to promote transparency, accountability, and integrity;
- Develop City services that will support Division Heads to improve data quality and make data findable, accessible, and interoperable through vocabulary and metadata programs, standards, tools, and best practices;
- Develop City services that improve data sharing and protection through privacy and access programs, standards, and best practices;
- Provide Divisions consultative corporate programs and services that embed legislatively required information and data lifecycle management and protection by design into their operations, services, technologies, 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](#);
- Develop and implement preservation policies, standards, procedures and strategies to ensure information with long-term and permanent retention periods remains useable throughout the information lifecycle;
- Collaborate with corporate partners to lead and promote Information Management and governance training and awareness, assisting and enabling Divisions to increase information and data governance capacity;
- Ensure the separation, segregation, and protection of information and data belonging to Accountability Officers and Elected Officials, where required;
- Preserve and provide access to the City's archival records regardless of medium and format;

- Provide privacy impact assessments, breach management, and access requests; and
- Provide Information Management and data governance oversight and guidance through business processes to support information and data authenticity, accessibility, findability, interoperability, usability, safety, and trustworthiness.

7.2 Chief Information Security Officer will:

- Proactively work with Divisions to assist with the development of security measures that align with City of Toronto cyber security policies and industry standards and best practices, to ensure authorized access to and appropriate use of City information and data;
- Provide leadership and vision for cyber security policies, infrastructure, and initiatives for the City, reflecting industry best practices;
- Proactively work with City Divisions and corporate partners to implement and enforce physical, policy, and technological controls to safeguard information and data;
- Collaborate with senior leadership, all levels of management, and corporate and Divisional partners to assist with the determination of acceptable level of risks and assess the design and effectiveness of risk mitigation approaches and/or solutions to mitigate the City's security risk exposure;
- Understand and articulate the impact of cyber security threats on data assets through cyber security assessments, including penetration testing and threat risk assessments;
- Investigate any access or security breach in City digital infrastructure, including, for example, the loss, inappropriate access to, or unauthorized disclosure of, the City's electronic records and information; and
- Have oversight over cyber security assessments, ensuring the achievement of City business objectives where business processes are dependent on technology.

7.3 Chief Technology Officer will:

- Provide strategic direction for technology, digital infrastructure, and electronic government service delivery;
- Design technology in an anticipatory and conscientious manner that considers and builds interoperability across solutions, technologies, and data streams by design;
- Provide oversight of the enterprise-wide adoption of on-demand cloud services for Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) through governance, compliance and security;
- Integrate Information Management, data governance, privacy, authentication, and access requirements by design into technology architectures, solutions, policies, standards, and implementation activities, in accordance with the

requirements of [Municipal Code Chapter 217, Corporate Records](#), [MFIPPA](#), and relevant City data governance and information management policies and standards, in both operational and capital projects and programs;

- Develop and maintain technology policies, standards, procedures, and architectures;
- Implement physical, policy, technological, and compliance controls to protect information and data;
- Enable Data Custodians, whether from Technology Services Division or within supported Divisions, to ensure the safe custody, transport, and storage of information and data, and implementation of business rules, understanding the technological and system architecture requirements to support data management activities defined by the Data Stewards;
- Provide consultation and services in the planning and design of enterprise or Divisional information and data storage infrastructure and hosting, whether on-premise or in cloud infrastructure (e.g., data centre, data lake, data warehouse, etc.);
- Empower Divisions to leverage location data for business decisions through Geographic Information System (GIS) programs, services, and tools;
- Aid Divisions in generating information and data to support better decision making through business intelligence and data analytics programs, services, and tools;
- Develop and maintain data infrastructure to accommodate legal holds and extraction (e.g., for litigation or FOI requests) and support management of information and data throughout their lifecycle;
- Provide and maintain an enterprise inventory of data repositories that captures all data storage systems and their usage;
- Provide services related to the design, modelling, and interoperability of data in enterprise or divisional systems; and
- Implement and support the City's [Open Data Policy](#), including managing an inventory of open and routinely disclosed data in compliance with City's [Records Retention By-laws](#).

7.4 Chief People Officer, People & Equity will:

- Collaborate with corporate partners to develop, implement, and monitor corporate strategies, policies, standards, and procedures in the areas of equity and data, inclusion, and human rights;
- 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 data in a consistent and equitable manner, aligning with information management requirements and best practices;

- In partnership with communities, lead the development of First Nations, Inuit, Metis Data Governance (FNIMDG) Framework and [Black Community Data Governance \(BCDG\) Framework](#) that supports, advances, and works to address the unique experiences of FNIM and Black communities, especially when it comes to historic and ongoing impacts of data and societal systems;
- Advance organizational capacity, drive common purpose and accountability through guidance, and the delivery of training, skill development, and awareness programs; and
- 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 FNIM, Black, and other equity-deserving groups.

7.5 Division Heads will:

- Promote openness, access, and transparency through collaboration and information sharing across their Division and with the public;
- Embed information and data governance in the culture, behaviour, and attitude of their staff
- Promote and address the principles of First Nations, Inuit, and Metis information and data governance and methods of FNIM engagement and guidance, through applicable strategies and frameworks, in how information and data are collected, protected, used, and shared. The First Nations principles of OCAP® (Ownership, Control, Access and Possession) provide a model for the City's approaches to FNIM data governance;
- Ensure their Division engages Black and other equity deserving communities in the development, collection, analysis, reporting, and use of information and data, and that disaggregated data is reported back to communities, aligning with the City's Black Community Data [Governance Framework](#);
- Promote information and data standardization, quality, protection, security, and integration in Divisional initiatives and programs.
- Ensure strategic planning occurs for information and data governance goals, targets, and outcomes in the Division, with accountabilities and monitoring practices outlined;
- Ensure the findability, accessibility, interoperability, reusability, ethical use, safety and security, authenticity, and integrity of information and data to meet operational, service delivery, and project needs;
- Manage, access, and use information and data in their Division in accordance with this policy and the [City of Toronto Act](#), [MFIPPA](#), [Chapter 217 of the Toronto Municipal Code](#), [Information Management Accountability Policy](#), [Protection of Privacy Policy](#), [Acceptable Use of Information Technology Assets Policy](#), [Remote Work Guideline](#), [Data for Equity Strategy](#), [Digital Infrastructure Strategic](#)

[Framework](#), and other relevant legislation and City policies, including future frameworks related to information and data governance;

- Manage data in their Division as Data Owners who are accountable for data assets within specific data domains and the appropriate sharing and usage of them;
- Assign Data Stewards and Data Custodians, as appropriate, within their Division;
- Consult with the City Clerk's Office, CIMS, before undertaking technology projects in order to embed legislated information management requirements;
- Communicate, implement, and support compliance with all information and data governance policies and standards established by the City Clerk, Chief Technology Officer, and Chief Information Security Officer in their Divisions;
- Designate Divisional staff to represent the Division, as appropriate, on corporate initiatives that impact how they collect, procure, manage, store, use, provide access to, publish, and dispose of City information and data;
- Ensure staff are aware of their responsibilities when managing information and data throughout their lifecycle;
- Ensure staff are aware of, and account for, the understanding that information and data are not neutral, but shaped by methodology, culture, and biases, in using them;
- Ensure the equitable use of data for decision-making within their Division by promoting and participating in data equity capacity building and training;
- Make information and data available in response to [Freedom of Information \(FOI\)](#) requests, in accordance with legislated timeframes;
- Restrict access to City information and data, including personal information, in accordance with the appropriate [information protection classification categories](#), to those individuals who require access in order to perform their duties and where access is necessary for the lawful administration of their business;
- Manage information and data in compliance with the City's [Records Retention By-laws](#) and other relevant City policies and legislation; and
- Ensure vendors, contractors, and third parties with access to City information and data are bound to comply with all applicable Information Management, records, data governance, privacy, and access policies and legislation.

7.6 All Employees will:

- 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;

- Review and comply with Information Management, information and data governance, recordkeeping, security, confidentiality, and privacy protection policies, standards, and practices;
- Foster a culture of openness and transparency through collaboration and lawful and ethical information and data sharing across Divisions;
- Inform themselves of their information and data governance obligations through City-offered education, including information management, privacy and data governance training, and skills development courses, as appropriate to their job duties;
- Limit the amount and type of information and data collected to what is needed for the identified purposes and specified lifecycle of the operation or project;
- Examine and understand the principles of First Nations, Inuit, and Metis data governance and methods of FNIM engagement and guidance, through applicable strategies and frameworks, in how information and data are collected, protected, used, and shared. The First Nations principles of OCAP® (Ownership, Control, Access and Possession) provide one model for the City's approach to respecting FNIM data governance;
- Ensure that Black and equity-deserving communities are engaged in the City's development, collection, analysis, reporting, and use of information and data and that disaggregated data is reported back to communities, in alignment with the City's [Black Community Data Governance Framework](#);
- Collaborate, engage, and share information and data with Black and equity-deserving communities, experts, and organizations to ensure the City moves towards information and data use that supports positive community outcomes and does not stigmatize, harm, or negatively impact Black and equity-deserving communities;
- Inform themselves, through applicable strategies and frameworks, that data is not neutral, but shaped by methodology, culture, and biases that must be accounted for when using data;
- Manage information and data in such a way that it provides concise, accurate, and complete evidence of the City's decisions, transactions, and activities, regardless of the communication methods (e.g., meetings, instant messaging, email, voice messaging, etc.) and ensure that information, records, and data are stored in an appropriate, City-approved repository;
- When appointed as Data Stewards, ensure the effective stewardship of data and represent data assets on behalf of Data Owners, as individuals who understand the business processes and data being produced within those processes;
- When appointed as Data Custodians, ensure the safe custody, transport, and storage of data, and the implementation of business rules;
- Manage information and data securely when using collaboration tools with internal and external parties; and

- Notify the appropriate management staff regarding identified gaps or areas of concern in privacy, information, and data management when collecting, using, managing, disclosing, and disposing of information and data within their purview.

8. Compliance

This Policy directs the City to be compliant with [MFIPPA](#), [Toronto Municipal Code, Chapter 217, Records, City](#), the [City of Toronto Act](#), and other laws applicable to information, data, records, and privacy accountabilities by:

- Ensuring City Divisions and Division Heads strategically plan, develop, document, and implement measures to manage and protect their information, data, and records. This can be accomplished through Divisional strategic planning and/or setting of performance objectives. Corporate Information Management Services (CIMS) is available to consult with Divisions on incorporating information and data governance accountabilities within their program and project planning.

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.

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

9. References

- [ARMA International. Information Governance Implementation Model \(IGIM\). Retrieved from: <https://www.arma.org/page/igim#>](#)
- City of Toronto, City Clerk's Office (2018). Acquisitions Policy for the City of Toronto Archives (2018). Retrieved from: <https://www.toronto.ca/city-government/accountability-operations-customer-service/access-city-information-or-records/city-of-toronto-archives/about-the-archives/policies-and-procedures/acquisition-policy-for-the-city-of-toronto-archives/>
- City of Toronto, City Clerk's Office (2021). Digital Preservation Policy. Retrieved from: <http://insideto.toronto.ca/clerks/policies/files/digital-preservation.pdf>
- City of Toronto, City Clerk's Office. City Data Governance and Information Management Glossaries. Retrieved from: <https://kb.intra.prod-toronto.ca/KB/index#>
- City of Toronto, City Clerk's Office. Common Data Elements for City Forms (2017). Retrieved from: <https://www.toronto.ca/wp-content/uploads/2017/08/97af-Common-Data-Elements-for-City-Forms.pdf>

- City of Toronto, City Clerk's Office. Information & Data Governance Framework (2024). Retrieved from: <https://insideto.toronto.ca/clerks/policies/files/information-data-governance-framework.pdf>
- City of Toronto, City Clerk's Office. Freedom of Information. Retrieved from: <https://www.toronto.ca/city-government/accountability-operations-customer-service/access-city-information-or-records/freedom-of-information/>
- City of Toronto, City Clerk's Office. Information Management Accountability Policy (2023). Retrieved from: <https://www.toronto.ca/wp-content/uploads/2018/07/8ec6-information-management-accountability-policy.pdf>
- City of Toronto, City Clerk's Office. Information Management Framework (2019). Retrieved from: <https://www.toronto.ca/wp-content/uploads/2019/12/8cba-Information-Management-Framework.pdf>
- City of Toronto, City Clerk's Office. Information Protection Classification Standard (2023). Retrieved from: <https://insideto.toronto.ca/clerks/policies/files/information-protection-classification-standard.pdf>
- City of Toronto, City Clerk's Office. Municipal Code Chapter 217, Records, Corporate (City) (2021). Retrieved from: http://www.toronto.ca/legdocs/municode/1184_217.pdf
- City of Toronto, City Clerk's Office. Protection of Privacy Policy (2014). Retrieved from: <https://www.toronto.ca/wp-content/uploads/2017/08/9023-ProtectionOfPrivacyFinalAODA.pdf>
- City of Toronto, City Clerk's Office. Responsible Record-Keeping Directive (2012). Retrieved from: https://www.toronto.ca/wp-content/uploads/2017/08/9741-Responsible-Record-Keeping-Directive-Final_1.pdf
- City of Toronto, People & Equity. Data for Equity Strategy (2020): Retrieved from: <https://www.toronto.ca/legdocs/mmis/2020/ex/bgrd/backgroundfile-158046.pdf>
- City of Toronto, Technology Services Division. Acceptable Use Policy (2018). Retrieved from: https://insideto.toronto.ca/itweb/policy/pdf/acceptable_use.pdf
- City of Toronto, Technology Services Division. Digital Infrastructure Strategic Framework (2022). Retrieved from: <https://www.toronto.ca/wp-content/uploads/2022/03/9728-DISFAcc2.pdf>
- DAMA International. Data Management Book of Knowledge (DAMA-DMBoK 2nd edition). Retrieved from: <https://www.dama.org/cpages/body-of-knowledge>
- International Standards Organization (ISO). ISO 38505-1: Information Technology - Governance of Data (2017). Retrieved from: <https://www.iso.org/standard/87195.html>

- Province of Ontario. Municipal Freedom of Information and Protection of Privacy Act (1990). Retrieved from: <https://www.ontario.ca/laws/statute/90m56>
- Province of Ontario. Personal Health Information Protection Act (2004). Retrieved from: <https://www.ontario.ca/laws/statute/04p03>
- The First Nations principles of OCAP® (Ownership, Control, Access, and Possession). OCAP® is a registered trademark of the First Nations Information Governance Centre (FNIGC). Retrieved from: <https://fnigc.ca/ocap-training/>

10. Policy Approval

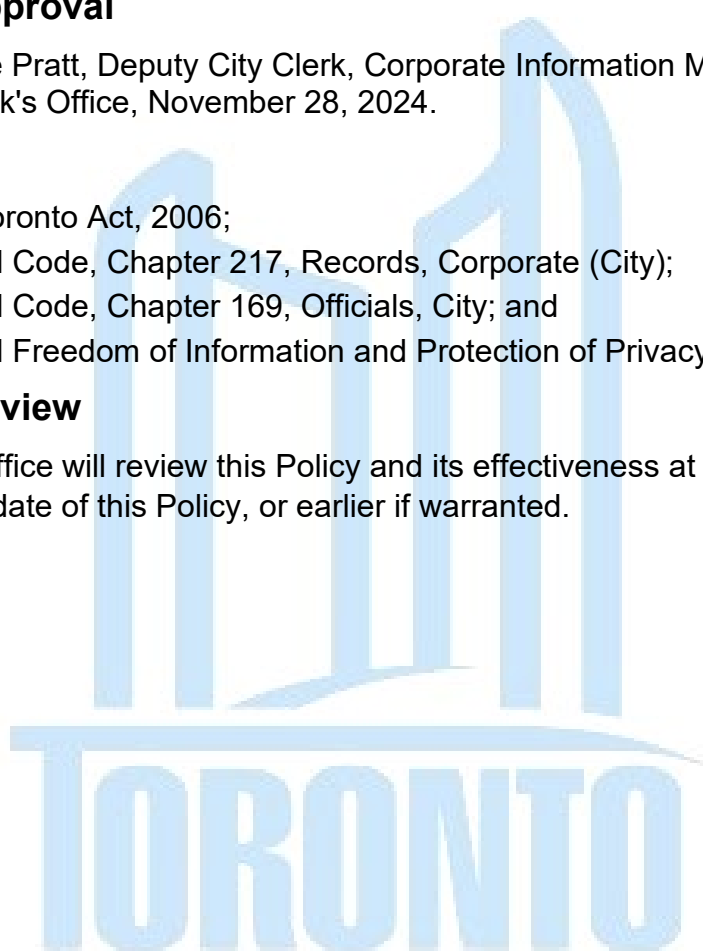
Provided by Kristie Pratt, Deputy City Clerk, Corporate Information Management Services, City Clerk's Office, November 28, 2024.

11. Authority

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

12. 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 A: Definitions

Terms within this policy are derived from the City's Information Management Glossary. The glossary provides definitions of key concepts in Information Management and related knowledge domains.

Business intelligence: A set of concepts, methods, and processes to improve business decision-making using any information from multiple sources that could affect the business and applying experiences and assumptions to deliver accurate perspectives of business dynamics.

Corporate partner: Corporate offices responsible for providing a broad range of programs and services to support Divisions. Includes the City Clerk's Office, the City Manager's Office, Technology Services Division, and Office of the Chief Information Security Officer.

Cyber security: The practices of security applied to digital infrastructure. Includes protection of physical digital infrastructure (like literal cables and servers) and non-physical digital infrastructure (like access and storage of data, limiting use of technologies, etc.)

Data: The raw material used to represent information, or from which information and records can be derived, represented as text, numbers, graphics, images, sound, or video.

Data attributes: An inherent fact, property, or characteristic describing an entity or object; the logical representation of a physical field or relational table column. A given attribute has the same format, interpretation, and domain for all occurrences of an entity. Attributes may contain adjective values (red, round, active, etc.).

Data classification (information protection classification): A classification category placed on systems, applications, repositories, and records controlling their sharing and disclosure, in line with applicable privacy legislation.

Data custodians: Individuals who understand the technological and system architecture requirements to support data management activities defined by the Data Stewards.

Data Custodians are responsible for the safe custody, transport, and storage of the data, and implementation of business rules.

Data entities: A classification of objects found in the real world described by the noun part of speech - persons, places, things, concepts, and events - of interest to the enterprise. Usually expressed in singular form.

Equity: understanding, acknowledgement and removal of barriers that prevent the participation of any individual or group, making fair treatment, access, opportunity, advancement, and outcomes possible for all individuals.

Information and Data Governance: The exercise of authority and control (planning, monitoring, and enforcement) over the management of information and data assets.

Data literacy: The ability to think critically about data in different contexts and examine the impact of different approaches when collecting, using, and sharing data and information.

Data owners: Individuals who are accountable for data assets within specific data domains with the ability to make and enforce decisions related to the data regardless of who collects or who manages it.

The Data Owner is responsible for the implementation of policies and guidelines that define the appropriate use of the data, ensuring that appropriate steps are taken to protect data, and ensuring compliance with relevant legislation.

Data quality: The degree to which data is accurate, complete, timely, consistent with all requirements and business rules, and relevant for a given use.

Data stewards: Individuals who understand the business processes and the data being produced within those processes. Data Stewards can represent the data assets on behalf of the Data Owners. Data stewards are often categorized as executive data stewards, business data stewards, or coordinating data stewards based on their day-to-day responsibilities.

Disaggregated data: Disaggregated data refers to data that is broken down and examined by socio-demographic groups such as Indigenous communities, gender, race, and neighbourhoods. Data that is broken down by socio-demographic groups can be used to identify and address differences between groups of Toronto residents.

Disposition: The final action with regard to records, including records destruction and transferring for permanent preservation.

Geographic Information Systems (GIS): Systems or tools for creating, storing, editing, analyzing, and managing geospatial data entities and associated attributes.

Information: Data that has been given value through assessment, interpretation, or compilation in a meaningful form.

Interoperability: The capacity of different information systems - which could come from different providers - to work together and share information without technical or legal restrictions.

Master data: The data that provides the context for business activity data in the form of common and abstract concepts that relate to the activity. It includes the details (definitions and identifiers) of internal and external objects involved in business transactions, such as customers, products, employees, vendors, and controlled domains (code values).

Metadata: Data describing context, content and structure of records and their management through time, and it can describe the properties of a document or file.

Personal Information: As defined in MFIPPA, “personal information” means recorded information about an identifiable individual, including:

1. Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual
2. Information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved
3. Any identifying number, symbol or other particular assigned to the individual
4. The address, telephone number, fingerprints, or blood type of the individual
5. The personal opinions or views of the individual except if they relate to another individual
6. Correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence
7. The views or opinions of another individual about the individual
8. 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

Privacy: A set of interests and rights that an individual has regarding his or her ability to control the collection, use, disclosure, and retention of his or her own personal information that is in the custody or control of a third party (including the City of Toronto). Privacy is not an absolute right in all situations. Personal information may be collected, used, disclosed, or retained without the consent of individuals where specific legislation permits.

Privacy by design: To build privacy and data protection, into the design specifications and architecture of information and communication systems and technologies at the beginning, in order to facilitate compliance with privacy and data protection principles.

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.

Reference data: Describes identifiers used to reference relevant particulars for highly complex transactions with multiple dependencies, entities, and contingencies. Includes values that give context to other master data and/or transactional data such as list of countries, industry sectors, classifications, etc.

Socio-demographic data: Describes personal characteristics and social identity. Characteristics such as age, language, race, First Nations, Inuit, Metis identity, Canadian-born or immigrant, disability, gender, sexual orientation, income, and place of residence are all examples of socio-demographic data.

Structured data: Machine readable information that is stored according to a pre-defined data model.

Transactional data: Relates to the transactions of the organization and includes data that is captured when a product is sold or purchased, or a service is paid for. Relates to transactions against financial master data objects. Day-to-day accounting and financial activities that are recorded against financial master data objects.

