Data Quality Policy

Policy No.: CIMS-018
Version No.: 1.0
Issued By: Corporate Information Management Services, City Clerk's Office
Approval Date: July 20, 2026
Subject: Data Governance, Information Management
Keywords: information, data, governance, privacy, records, data quality

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 & Business Units:

- Corporate Information Management Services, City Clerk's Office
- Toronto Cyber Security
- People & Equity Division
- 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) 803-9140
Kristie.Pratt@toronto.ca

Table of Contents

1. Introduction

High-quality City data underpins effective decision-making, transparent service delivery, and accountability to the public. When data is accurate, complete, consistent, timely, and reliable, the City can deliver programs efficiently, support evidence-based decision making, report with confidence, and uphold public trust. All information and data collected, created, used, stored, and shared by the City of Toronto are corporate assets of the City that must be managed and maintained as business records while upholding Data Quality in service delivery.

The Data Quality Policy (DQP) establishes the City's commitment to maintaining and improving the quality of its data assets. It defines Data Quality dimensions, roles, responsibilities, and governance practices to ensure that data is fit for purpose and aligned with organizational, legislative, operational, and public interest needs. This Policy complements and operationalizes the commitments outlined in the Information and Data Governance Policy (IDGF) and Framework by detailing the quality management aspect of information governance.

Data Quality refers to the degree to which data is fit for its intended use and can be trusted to support City services, operations, reporting, analytics, and decision-making. It is evaluated through dimensions such as accuracy, completeness, consistency, timeliness, validity, reliability, relevance, traceability, and uniqueness. In a public sector context, Data Quality also includes considerations related to fairness, representativeness, transparency, and the responsible use of data to support equitable and evidence-based decision making. City data includes financial and non-financial master data that provides an authoritative source of key business entities, transactional data generated through business operations, reference data that supports consistency, and associated metadata.

Examples of City data may include:

- Socio-demographic data used to support equitable policy and service planning;
- Operational and service delivery data;
- Financial asset and infrastructure data;
- Reporting and analytical datasets; and
- Externally acquired data used for operational, analytical, regulatory, or public reporting purposes.

This Policy provides a unified framework for managing Data Quality across the information and data lifecycle – from throughout the data lifecycle, including data creation, collection, storage, use, sharing, retention, and disposition. It defines the dimensions, principles and practices that support consistent and effective management of data used for analytics, reporting, operational processes, and decision-making. This policy also ensures that City Divisions and employees understand their roles in

assessing, maintaining, and improving Data Quality. Consistent and interoperable data also supports the City's ability to make information more accessible and usable, where applicable.

By implementing this Policy, the City will strengthen the reliability of its corporate data assets, reduce operational risks and inefficiencies caused by poor-quality data, improve service delivery through consistent Data Quality practices, and promote an organizational culture of stewardship and accountability for City data assets. High-quality data also supports evidence-based decision making and the responsible use of emerging technologies, including advanced analytics, automation, and AI-enabled tools.

2. Purpose

The purpose of this Policy is to establish a consistent enterprise approach for managing and improving Data Quality across the City of Toronto by defining core Data Quality dimensions, accountabilities, and governance practices that support trusted, reliable, and fit-for-purpose data. This includes:

- Establishing an enterprise framework for managing Data Quality across the data lifecycle, including data creation, collection, use, storage, sharing, retention, and disposition.
- Defining core Data Quality dimensions, responsibilities, and practices that support Divisions in assessing, monitoring, and improving Data Quality based on operational and business needs.
- Enabling comparability, traceability, and reliability of data used for analytics, reporting, and Open Data initiatives.
- Supporting compliance with applicable legislation, standards, and City policies by embedding requirements into the recommended Data Quality processes.

2.1 Strategic Context

This Policy supports alignment with corporate data governance strategies, standards, and frameworks, including:

- **Information and Data Governance Framework and Policy**: Establish a corporate approach to managing data, including accountability and decision-making authority across Divisions. Data Quality management is an integral component of the following Information and Data Governance Framework domains:
    - Data Lifecycle Management – ensuring quality through the data lifecycle, from creation to disposition;

  - Metadata and Standards – promoting interoperability through consistent definitions and data formats;
  - Information Security and Privacy – maintaining data integrity and accuracy while protecting confidentiality;
  - Governance and Accountability – defining roles and processes for ongoing measurement, review, and improvement of data.
- **Open Data Policy**: Establishes quality and privacy standards for City data while promoting its public access and use.
- **Data for Equity Strategy**: Ensures socio-demographic and disaggregated data is accurate, contextual, and informed by, and representative of, community priorities when used in City business.
- **Metadata Standards**: Support Data Quality through consistent, structured rules for data descriptions, ensuring accuracy, completeness, and interoperability across systems.

Together, these frameworks establish the policy foundation and mandate for trusted, secure, and high-quality data to advance evidence-based policy, service excellence, and equity-informed outcomes for the people who live, work and access services in Toronto. The Data Quality Policy focuses on operationalizing the City's Data Quality mandate through defined principles, responsibilities, and governance practices.

2.2 Legislative and Policy Alignment

This Policy also aligns with the following legislation and City policies:

1. Municipal Freedom of Information and Protection of Privacy Act (MFIPPA);
2. Personal Health Information Protection Act (PHIPA);
3. City of Toronto Act, 2006 — sets records retention and accountability requirements;
4. Information and Data Governance Policy (CIMS-016) — outlines the City's framework for governing information and data;
5. Information Management Accountability Policy — defines corporate responsibilities for managing information and data assets;
6. Toronto Municipal Code, Chapter 217, Records, Corporate (City) — focuses on managing information and records and specific records retention requirements;
7. Protection of Privacy Policy — sets the requirements for privacy protection and the public service responsibility for safeguarding data containing personal information; and
8. Information Collection Policy / Personal Information: Collection, Use and Disclosure Guideline — provides direction on collecting, managing and protecting personal and sensitive information from members of the public.
9. Responsible Recordkeeping Directive – codifies legislated recordkeeping accountabilities for City Divisions.

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), FAIR (Findable, Accessible, Interoperable, Reusable) guiding principles for the management of data across different domains, and the International Standards Organization (ISO) 38505 – IT – Governance of Data.

3. Scope

This Policy applies to structured and semi-structured data collected, created, maintained, shared, acquired, or reported by the City of Toronto in support of municipal business, service delivery, analytics, reporting, and decision-making.

This includes data managed within City-operated systems, shared across Divisions, acquired from external organizations, or provided through third-party service providers where the City has responsibility for the use, management, reporting, or stewardship of the data.

Responsibility under this Policy applies to the management, validation, monitoring, and appropriate use of data once it is within the City's custody, control, or operational use.

Much of this data may constitute City business records and must be managed in accordance with Municipal Code, Chapter 217, Records, Corporate (City), requiring appropriate retention and disposition of City records.

Unstructured data, including audio, video, image, and free text content, may not be fully governed through all Data Quality dimensions outlined in this Policy. City Divisions are encouraged to apply appropriate Data Quality practices to unstructured data where operationally feasible and aligned with business requirements.

This Policy applies Data Quality principles across the data lifecycle, including data creation, collection, storage, processing, integration, sharing, retention, archival preservation, and disposition. Different Data Quality dimensions may have varying levels of relevance depending on the stage of the data lifecycle and the operational context in which the data is used.

Divisions are encouraged to prioritize the application of this Policy to high-value, high-risk, shared, regulatory, operational, analytical, or publicly reported datasets based on business impact, service delivery requirements, legal obligations, and operational risk.

4. Application

This Policy applies to all City of Toronto Divisions and employees, volunteers, contractors, consultants, third-party service providers, and subcontractors who collect, create, manage, share, report on, or use City data in support of government business and service delivery.

Third-party vendors, contractors, consultants, and service providers acting on behalf of a City Division are expected to implement applicable Data Quality requirements, standards, and controls as defined through divisional business processes, contractual agreements, system requirements, or operational procedures.

Corporate partners referenced throughout this Policy include corporate offices that provide governance, technology, security, information management, advisory, or operational support to Divisions. This includes the City Clerk's Office, the City Manager's Office, Technology Services Division, People & Equity, and Toronto Cyber Security.

Divisions remain accountable for managing the quality of data used within their operational environments, with support from applicable corporate governance, information management, privacy, cybersecurity, and technology partners.

5. Data Quality Dimensions

The City commits to promoting and maintaining the following Data Quality dimensions to support trustworthy, usable, and fit-for-purpose data across operational, analytical, reporting, and service delivery environments.

Data Quality dimensions provide a standardized framework for evaluating the quality, reliability, and fitness of City data throughout its lifecycle. Different dimensions may carry different levels of importance depending on the nature of the data, operational context, business use, legislative requirements, and associated risk.

The following dimensions establish foundational expectations for assessing, managing, monitoring, and improving Data Quality across City data environments:

5.1 Accuracy

Data should accurately reflect the real-world entities, activities, or events it represents in a manner appropriate to its intended use and operational context. This includes ensuring that:

- Controls are implemented to prevent and detect errors during data entry, collection, transfer, integration, and transformation.
- Validation and reconciliation procedures, supported by appropriate business rules and systems controls where feasible, help identify and correct inaccurate, incomplete, or inconsistent data values.
- Divisions mitigate the potential business, financial, or reputational impacts of inaccurate data based on how the data is used.

5.2 Completeness

Data should contain the elements necessary to support its intended operational, analytical, reporting, or legislatively defined use. This includes confirming that:

- Divisions identify and correct missing, partial, or null values where appropriate, while maintaining sufficient auditability and accountability.
- Divisions define and monitor completeness expectations and thresholds for data elements that are critical to operational, reporting, legislative, or service delivery requirements.
- Divisions determine which data elements are essential to support business process, reporting, or regulatory requirements.

5.3 Consistency

Data should maintain an appropriate level of consistency across systems, business processes, integrations, and reporting environments based on operational requirements and data sharing needs. This includes ensuring that:

- Naming conventions, reference codes, data types, and formats align with established corporate standards where applicable and are consistently applied within and across integrated or shared datasets.
- Divisions review and address conflicting system values, duplicate records, or inconsistencies through appropriate reconciliation, stewardship, or operational processes.
- Consistency expectations account for cross-divisional data sharing, integration, and enterprise reporting needs.

5.4 Timeliness

Data should be captured, updated, and made available within timeframes appropriate to its intended use, operational requirements, and service delivery needs. This includes ensuring that:

- Divisions define updates cycles, refresh expectations, or availability requirements appropriate to the operational nature and use of the dataset.
- Delays in data updates are documented and addressed through process improvements.
- Update or refresh cycles reflect how frequently data is required to support decisions, services, or regulatory and/or legislative obligations.

5.5 Validity

Data should conform to applicable business rules, formats, standards, and validation requirements relevant to its operational context and intended use. This includes confirming that:

- Validation rules are embedded in data collections systems to prevent entry of invalid or non-conforming data.
- Metadata specify the acceptable range or domain of each attribute.

- Validity expectations are defined with consideration for system constraints, data sources, and the context in which the data is used.

5.6 Reliability

Data should be dependable, transparent, and sufficiently verifiable to support operational, analytical, reporting, and decision-making activities. This includes maintaining practices that ensure:

- Divisions consider the reliability of data sources when using data for operational decisions, analysis, or public reporting.
- Data lineage is documented to trace its origin, transformation, and use.
- Quality assurance procedures are in place to ensure reproducibility of data outputs.

5.7 Relevance

Data must be appropriate and useful for the purpose for which it is collected or maintained. This includes regularly confirming that:

- Divisions periodically review the data they collect, maintain, share, or use to confirm continued business relevance and operational value.
- Outdated or redundant data is archived or retired in accordance with retention by-laws.
- Data relevance is periodically reassessed as business needs, services, or programs evolve.

5.8 Traceability

Data should be traceable through its lifecycle to support transparency, accountability, operational understanding, auditability and appropriate stewardship. This includes ensuring that:

- Every dataset or data asset includes a unique identifier to distinguish it from similar data objects.
- Data lineage and supporting metadata document, where appropriate, the origin, movement, transformation, collection context, use, and access history of data to support transparency, accountability, and verification that data has been accessed or modified by authorized individuals.
- Traceability considerations reflect the need to support transparency, accountability, and issue resolutions for high-impact data uses.

5.9 Uniqueness

Data should be managed in a manner that reduces unnecessary duplication and supports the consistent identification of records, entities, or assets where appropriate. This includes ensuring that:

- Unique identifiers or business keys are used where appropriate to distinguish records or entities.
- Duplicate records are identified, reviewed, and managed through operational or stewardship processes.
- Divisions consider the operational and reporting impacts of duplicate or fragmented data across systems and processes.

These Data Quality dimensions align with recognized industry standards and best practices, including the DAMA Data Management Body of Knowledge (DAMA-DMBOK), FAIR (Findable, Accessible, Interoperable, Reusable), and the City's Information and Data Governance Framework. Together they support a consistent and risk-informed approach to managing Data Quality across diverse operational and service delivery environments.

6. Data Quality Management Framework

The Data Quality Management Framework establishes the City's structured and risk-informed approach to defining, assessing, monitoring, and improving Data Quality. The Framework provides guidance for applying Data Quality principles and practices across divisional contexts while supporting operational flexibility, legislative requirements, service delivery needs, and diverse data environments throughout the data lifecycle.

The Framework aligns with recognized industry standards and best practices, including DAMA-DMBOK (Data Management Body of Knowledge), FAIR principles, and the City's information and Data Governance Framework, while remaining adaptable to the City's operational diversity and governance structure.

6.1 Framework Components

Divisions are encouraged to maintain appropriate metadata, data definitions, and business terminology to support consistent interpretation and management of data. The Data Quality Management Framework is composed of the following key components:

1. **Data Quality Dimensions**: Section 5 of this policy defines core Data Quality dimensions – accuracy, completeness, consistency, timeliness, validity, reliability, relevance, traceability and uniqueness – which support the foundation for assessing and understanding Data Quality across operational and analytical contexts.
2. **Data Quality Metrics**: Quantitative and qualitative measures are used to evaluate the quality of data assets. Examples may include error rates, completeness measures, duplication trends, refresh cycle adherence, reconciliation outcomes, or other operationally relevant indicators.
3. **Data Quality Controls**: Preventive, detective, and corrective controls should be implemented where appropriate to support Data Quality throughout data collection, transformation, integration, reporting, and operational use. These

include validation rules, referential integrity checks, reconciliation routines, and audit trails.

4. **Monitoring and Reporting**: Divisions should periodically monitor and review Data Quality using business-defined measures, operational indicators, or applicable Key Performance Indicators (KPIs) appropriate to their operational context and risk profile. Results should be analyzed to identify trends, recurring issues, and opportunities for improvement.
5. **Issue Management and Remediation**: Data Stewards, Data Owners, and operational teams may support remediation activities in alignment with established governance responsibilities and operational processes.
6. **Continuous Improvement:** Divisions are encouraged to incorporate Data Quality improvement initiatives into business and technology projects. Divisions are encouraged to share lessons learned, best practices, and improvement opportunities through governance forums, collaboration channels, or communities of practice where appropriate.

6.2 Data Lifecycle and Quality Integration

Data Quality considerations should be incorporated throughout the data lifecycle in a manner appropriate to the operational context, business requirements, legislative obligations, and risks associated with the data.

The following examples illustrate common Data Quality management activities that Divisions may consider when managing data throughout its lifecycle. Not all activities will apply equally across all datasets, systems, operational environments, or service delivery contexts.

Data Lifecycle Stage	Data Quality Activities
Creation and Collection	Apply validation rules, define required fields where appropriate, and capture relevant metadata at source where feasible. Define required data elements, metadata requirements, and validation rules prior to or during data collection, where appropriate, to support consistent and reliable data capture.
Storage and Maintenance	Monitor Data Quality indicators and support consistency across systems where operationally required.
Usage and Sharing	Validate data suitability before operational, analytical, reporting, or public use where appropriate.
Retention and Archiving	Support integrity, retention, accessibility, and traceability requirements for archived data.
Disposition	Retain appropriate metadata to support accountability, transparency, auditability, or operational requirements.

These lifecycle based practices align with the Information and Data Governance Framework and Records Retention By-Laws, ensuring that data remains fit for purpose throughout its existence. Where data are defined as records, they must be managed in accordance with Municipal Code, Chapter 217, Records, Corporate (City).

The following examples illustrate common Data Quality management practices aligned with industry frameworks such as DAMA-DMBOK. Divisions may adopt or adapt these practices based on operational requirements, governance maturity, legislative obligations, system capabilities, and business priorities.

Lifecycle Stage	Key Data Quality Activities	Description
Planning	Define Data Quality Requirements	Establish standards for accuracy, completeness, validity, and timeliness. Document rules and thresholds for acceptable quality.
	Develop Data Quality Metrics	Identify Division-specific / business-specific KPIs for measuring quality (e.g., % of records containing errors, timeliness of data updates, or other business-defined measures).
	Implement Governance Framework	Assign roles and responsibilities for monitoring and enforcing quality.
Creation and Collection	Validate Incoming Data	Check for accuracy, completeness, and validity during ingestion. Flag non-compliant data early.
	Apply Data Profiling	Analyze source data to detect anomalies, duplicates, and missing values.
	Standardize Formats	Ensure data conforms to predefined formats and business rules.
Storage and Maintenance	Monitor Data Quality Continuously	Use automated checks for consistency, uniqueness, and integrity during updates.
	Correct Data Errors	Implement cleansing processes for inaccurate or incomplete records.

	Synchronize Across Systems	Ensure consistency between integrated systems and master data.
Usage	Track Timeliness and Accuracy	Validate that data is current and reliable for decision-making.
	Apply Business Rules	Enforce rules for data usage to maintain integrity and compliance.
	Assess fitness for Analytics / Business Intelligence	Profile data for analysis readiness, measure dimensions like accuracy and generate Data Quality reports for decision-making.
	Audit Data Quality	Perform periodic audits to ensure adherence to standards.
	Usage stage	Ensure Data Quality is maintained when data is shared internally or externally, and that appropriate metadata accompanies shared data where applicable.
Retention and Archiving	Preserve Data Integrity and Provenance	Ensure archived data remain complete and accurate for compliance.
	Apply Retention Policies	Validate that data meets legal and retention requirements outlined in Toronto Municipal Code, Chapter 217 (Records).
	Document Metadata	Maintain metadata for context and traceability of archived data.
Disposition	Validate Disposal Process	Confirm that deletion does not compromise remaining Data Quality.
	Remove Redundant Data	Eliminate duplicates and unnecessary records securely.
	Update Metadata	Record disposal actions for audit and compliance purposes.

6.3 Data Quality Assessment and Maturity

Divisions are encouraged to assess and improve their Data Quality capabilities using maturity-based approaches appropriate to their operational environment, governance structure, and available resources. Maturity assessments may be used to support continuous improvement planning, identify capability gaps, and guide the evolution of divisional Data Quality practices. Divisions may use maturity-based approaches to support continuous improvement planning, identify capability gaps, and guide the evolution of Data Quality management practices appropriate to their operational environment.

The following maturity characteristics are illustrative examples intended to support divisional self-assessment and continuous improvement activities.

Maturity Level Description

Initial	Ad-hoc Data Quality practices, limited awareness of standards.
Developing	Some control in place; Data Quality issues managed reactively.
Defined	Documented processes and role-based responsibilities established.
Managed	Quality metrics and dashboards in use; proactive monitoring and performance tracking established.
Optimized	Continuous improvement embedded within governance practices.

6.4 Key Performance Indicators (KPIs)

To enable comparability and accountability, the following examples illustrate common indicators that Divisions may use to assess and monitor Data Quality performance based on operational needs, business priorities, legislative requirements, and risk considerations.

The following indicators are illustrative examples only and may be adapted, expanded, or prioritized by Divisions based on operational context, risk considerations, legislative requirements, and business objectives.

Indicator	Definition	Illustrative Examples
Accuracy Rate	Degree to which data correctly reflects the real-world object or event	% of records verified as accurate
Completeness Rate	Percentage of required data fields populated	% of mandatory fields completed
Consistency Score	Level of uniformity across systems and datasets	Duplicate record trends, reconciliation variances, or cross-system inconsistencies.

Timeliness Index	Currency of data relative to its intended use	Alignment of refresh cycles or availability timelines with operational requirements.
Validity Score	Conformance with defined rules or formats	% of entries matching data standards
Reliability Measure	Stability and reproducibility of data outputs	Reliability of outputs, repeatability of results, or frequency of identified anomalies.

Divisions may define additional measures, thresholds, or operational indicators aligned with their business context, governance requirements, and service delivery objectives.

6.5 Tools and Technology Enablement

Divisions may leverage enterprise or divisional tools, technologies, and metadata management capabilities (such as the Taxonomy and Vocabulary Management Solution) to support Data Quality management activities where appropriate and available.

Technology adoption and implementation approaches remain subject to operational requirements, enterprise architecture considerations, procurement processes, funding availability, and divisional priorities.

These tools can support:

- Data profiling and quality assessment;
- Metadata management, lineage documentation, and traceability support where operationally required;
- Monitoring, reporting, visualization, and analytical support for Data Quality activities;
- Integration with the City's corporate data catalogue and reporting systems; and
- Consistent classification, taxonomy, and vocabulary management to improve data understanding and reuse.

7. Roles and Responsibilities

Effective Data Quality management requires collaboration and shared accountability across business, operational, technical, and governance functions. Roles identified in this Policy align with the City's Information and Data Governance Policy (IDGP) and

Data Accountability Framework and support a coordinated approach to maintaining Data Quality throughout the data lifecycle.

Divisions retain accountability for operational Data Quality within their business processes, systems, and service delivery functions, while corporate governance functions provide enterprise guidance, standards alignment, advisory support, governance coordination, and enabling capabilities.

City Clerk:

The City Clerk's Office's Corporate Information Management Services (CIMS) Unit provides corporate leadership, coordination, guidance, and governance support for information and data management practices across the City. CIMS, as the Information Management and Data Governance delegate of the City Clerk:

- Exercises 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.;
- Directs 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;
- Supports Divisions through corporate programs, guidance, standards, tools, and best practices that promote Data Quality, metadata management, accessibility, interoperability, and responsible data governance practices;
- Develops City services that improve data sharing and protection through privacy and access programs, standards, and best practices;
- Provides advisory services, guidance, and corporate coordination to support Divisions in implementation data governance and Data Quality practices, including connecting Divisions with relevant corporate initiatives where appropriate;
- Provides guidance, awareness resources, and advisory support related to Data Quality management practices and governance expectations;
- Supports monitoring, reporting, and continuous improvement activities related to the implementation of this Policy; and
- Coordinates the integration of Data Quality management into broader information and data governance initiatives.

Division Heads:

Division Heads are accountable for supporting Data Quality management practices within their operational areas, including ensuring:

- Divisional data management practices align with this policy, applicable corporate standards, governance expectations, and operational requirements;
- Appropriate governance, stewardship and accountability responsibilities are identified and documented where operationally required;
- Adequate resources and controls are in place for data validation, monitoring, and corrective actions; and
- Data Quality considerations are integrated into divisional business processes, system design, and data sharing arrangements.

Chief Information Security Officer (CISO):

- Supports alignment between Data Quality management practices and corporate cybersecurity, privacy, and information protection requirements;
- Provides oversight to safeguard the integrity, confidentiality, and reliability of City data within systems and digital services; and
- Supports the implementation of security controls and monitoring practices that protect the integrity of City data assets.

Chief Technology Officer (CTO):

- Supports enterprise technology architecture, platforms, and infrastructure capabilities that enable effective data management and quality practices;
- Provides oversight for systems and applications that create, store, transform, or exchange City data; and
- Supports integration of Data Quality requirements into enterprise architecture, system governance, and technology standards.

Chief People Officer (CPO):

- Supports workforce awareness and capacity related to responsible data management and Data Quality practices**;**
- Promotes alignment between organizational policies, training, and workforce practices and the City's Data Quality objectives; and
- Supports workforce awareness and organizational capability related to responsible data management and Data Quality practices.

Chief Communications Officer:

Supports the use and sharing of trusted, accurate, and appropriately governed City information in corporate communications by:

- Promoting the use of authoritative and approved data and data sources in corporate communications to staff and the public via social media, Toronto.ca, and other forums and formats.
- Working with the City Manager's Office, Division Heads, Divisional Program Managers, Project Directors and subject matter experts to ensure that

information communicated publicly is accurate, consistent, and aligned with corporate messaging.
- Collaborating with data owners and subject matter experts to resolve significant information accuracy or reliability issues that may affect corporate communications or the City's reputation.

All Employees:

City Employees who create, collect, manage, analyze, or use City data contribute to maintaining Data Quality within their operational responsibilities. As Data Consumers, employees rely on data for decision-making and service delivery and therefore play an essential role in identifying and preventing Data Quality issues.

Employees are expected to:

- Accurately enter and update data in City systems;
- Follow established data entry standards, metadata guidelines, naming conventions, and validation procedures;
- Support appropriate Data Quality and classification practices when contributing to analytical, reporting, automation, or AI-enabled processes,
- Report data errors or anomalies to their supervisors or designated Data Stewards; and
- Participate in training and awareness programs related to Data Quality and governance.

8. Data Management Roles and Responsibilities

This section outlines data management-specific roles that support consistent, accountable, and operationally appropriate Data Quality management practices. Data Owners, Data Stewards, and Data Custodians each hold specific responsibilities that collectively ensure data remains accurate, reliable, and fit for purpose throughout its lifecycle.

The following data management roles build on the Information and Data Governance Policy (IDGP) by outlining more detailed responsibilities specific to maintaining and improving Data Quality across the data lifecycle**:**

Data Owners:

Data Owners hold primary accountability for the strategic value, quality, and use of data within their Division or business unit. They are responsible for:

- Supporting the Data Quality, reliability, and fitness for purpose of data within their assigned operational or business domain;
- Establishing operational rules, validation expectations, and quality thresholds appropriate to business needs and risk considerations;

- Authorizing and overseeing corrective actions to address Data Quality issues;
- Ensuring alignment of divisional data with enterprise standards and metadata definitions; and
- Supporting data stewardship and custodianship activities as part of broader governance processes.

Data Stewards:

Data Stewards act as operational leads for maintaining Data Quality within their assigned subject areas. They are responsible for:

- Implementing quality controls and validation rules in collaboration with technical and business teams;
- Supporting monitoring and issue identification related to Data Quality dimensions such as accuracy, completeness, consistency, and validity;
- Defining processes for labelling data and supporting consistent classification, labelling, and metadata management practices;
- Documenting metadata, lineage, and business definitions to support traceability;
- Identifying and escalating data issues to Data Owners and Division Heads for resolution; and
- Participating in Data Quality reviews, audits, and improvement initiatives.

Data Custodians:

Data Custodians are responsible for the technical management of systems and environments where data resides within their business unit or Division(s). They are responsible for:

- Supporting technical controls, validation mechanism, and system capabilities that help maintain Data Quality and integrity;
- Ensuring secure, authorized access to data consistent with privacy and security policies;
- Maintaining audit logs and change histories for data assets; and
- Supporting technical enablement for data profiling, monitoring, reporting, and quality management activities where feasible.

Cross-functional Collaboration:

Divisions should collaborate across business, operational, technical, and governance functions to support consistent and effective data management practices.
This includes:

- Collaborating with Technology Services Division (TSD) and governance partners on system capabilities, controls, architecture, and accountability considerations related to Data Quality management; and
- Working with CIMS' Records Services unit to ensure that data retention and disposition align with recordkeeping and lifecycle requirements.

9. Implementation

The effective implementation of the Data Quality Policy relies on divisional accountability. Divisions are responsible for supporting the implementation of this Policy through operational practices, procedures, governance activities, and business processes appropriate to their operational environment and data maturity.

Phase 1 – Foundational Alignment and Standardization

- Review of divisional Information and Data Governance structures and accountability practices to support alignment with this Policy and related governance frameworks.
- Identification and alignment of divisional datasets, metadata, or information assets with relevant corporate data domains, classifications, or governance structures where applicable.
- Development or adoption of consistent Data Quality definitions, metrics, validation practices, and governance expectations appropriate to business needs.
- Establishment of metadata, classification, taxonomy, and labelling practices that support searchability, interoperability, analytics, automation, and AI enabled processes, while maintaining appropriate business context, traceability, and lifecycle transparency.

Phase 2 – Monitoring and Reporting

- Development of monitoring, reporting, or KPI mechanisms appropriate to divisional operational and governance requirements.
- Periodic assessment, monitoring, remediation, or improvement activities related to Data Quality management.

Phase 3 – Continuous Improvement

- Incorporation of lessons learned and operational feedback into governance, procedural, and improvement activities.
- Exploration and enhancement of system capabilities, automation opportunities, and quality management practices where feasible.
- Cross-divisional sharing of best practices through the Data Governance Community of Practice (DG CoP).

9.2 Compliance

All City Divisions and programs, and City employees, volunteers, third-party vendors, and contract employees, including sub-contractors, hired by the City of Toronto are expected to align with and support the principles, requirements, and governance expectations outlined in this Policy, as applicable to their operational responsibilities.

Implementation approaches may vary across Divisions based on operational mandates, governance maturity, available resources, and legislative obligations.

- **Awareness and Training:** City Clerk's Office, in collaboration with TSD, may provide guidance, awareness resources, advisory support, or governance tools to assist Divisions in understanding and applying this Policy.
- **Periodic Review:** City Clerk's Office may support governance reviews, maturity assessments, or continuous improvement activities related to Data Quality management practices.
- **Reporting:** Divisions may participate in governance reporting, quality assessments, or improvement activities appropriate to operational and business requirements via the City's Data Governance Community of Practice.

9.3 Policy Review and Maintenance

This Policy will be reviewed periodically, or sooner if required due to legislative, organizational, operational, or technological changes. CIMS will coordinate review activities, engage relevant stakeholders and governance partners, and recommend updates to maintain the continued relevance and effectiveness of the Policy.

10. Policy Approval

Provided by Kristie Pratt, Deputy City Clerk, Corporate Information Management Services, City Clerk's Office July 20, 2026.

11. References

The following corporate documents, frameworks, standards, legislation and regulatory references provide context, authority, and guidance in relation to this Policy, and serve as best-practice foundations for implementing, assessing, and continuously improving Data Quality management across the organization:

11.1 Corporate Policies and Frameworks

- Information and Data Governance Policy – Establishes the overarching governance structure for managing the City's information and data assets.
- Information and Data Governance Framework – Defines the governance domains, principles, and accountability structure for City-wide data management.
- **Data Accountability Framework** – Describes divisional roles and responsibilities for information and data stewardship.

- **Information Management Accountability Policy** – Outlines employee responsibilities for managing information ethically, securely, and effectively.
- **Open Data Policy** – Promotes the proactive release of high-quality data to the public in support of transparency and innovation.
- **Data for Equity Strategy** – Ensures data is collected, analyzed, and shared in a way that supports equitable outcomes across communities.

11.2 Legislative and Regulatory References

- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Personal Health Information Protection Act (PHIPA) (applicable to Divisions and units that collect, use, disclose, or programs that collect, use, disclose, or manage personal health information in accordance with legislative requirements)
- City of Toronto Act, 2006
- Archives and Recordkeeping Act, 2006
- Accessibility for Ontarians with Disabilities Act (AODA)
- Records Retention By-Law (Municipal Code Chapter 217)
- Protection of Privacy Policy

11.3 Industry Frameworks and Standards

- DAMA-DMBOK – Data Management Body of Knowledge
- ISO 8000 – Data Quality Standards
- ISO/IEC 11179 – Metadata Registries
- FAIR Data Principles (Findable, Accessible, Interoperable, Reusable)
- Government of Canada – Data Quality Guidelines

Appendix A: Definitions

Term	Definition
City Data	Data, records, metadata, or information assets created, collected, received, maintained, shared, or used by the City in support of programs, services, operations, decision-making, reporting, legislative obligations, or business activities, regardless of format or system.
Accuracy	The degree to which data correctly describes the real-world object or event it represents.
Completeness	The extent to which all required data is present for a given purpose.
Consistency	The uniformity and coherence of data values across systems, reports, and business processes.
Data Consumer	Any individual or system that uses data to perform business tasks—examples include analysts, product teams, business users, downstream applications, and even automated processes. They do not create or manage data, but they rely on it to produce insights, make decisions, or deliver services.
Data Custodian	The individual or group responsible for the technical environment that stores or processes City data.
Data lifecycle	The sequence of activities through which data is planned, created, collected, stored, processed, integrated, used, shared, retained, and ultimately disposed of in accordance with business, legislative, operational, and governance requirements.
Data Owner	The senior business role accountable for the overall quality, compliance, and use of data within a defined domain.
Data quality	The overall fitness of data to serve its intended purpose in operations, decision-making, and reporting.
Data quality dimensions	Standardized criteria used to assess quality, such as accuracy, completeness, timeliness, and consistency.
Data quality management	The coordinated activities, processes, and governance practices used to assess, maintain, monitor, and improve data quality throughout the data lifecycle.
Data Steward	The role responsible for supporting the operational management, coordination, monitoring, and improvement of data quality within an assigned subject area or domain.
Division	An organizational unit within the City of Toronto responsible for specific operational or service functions.

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.
Critical Data Elements	Data elements identified by a division or business area as particularly important to operational processes, reporting, compliance, decision-making, public service delivery, or risk management
Information and Data Governance Framework	The City's overarching framework for managing data and information governance activities.
Metadata	Descriptive information about data that provides business context, meaning, structure, classification, lineage, ownership, or technical characteristics (e.g., source, format, ownership).
Personal Health Information	Personal Health Information is defined as identifying • information about an individual in oral or recorded form, that is in the custody or control of a Health Information Custodian (HIC), if the information relates to the physical or mental health of an individual, including information that consists of a person as a provider of health care to the individual • relates to the providing of health care to the individual including identification of a person as a provider of health care (e.g., physician's name) to the individual • is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual • relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual • relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance • is the individual's health number, or identifies an individual's substitute decisionmaker
Relevance	The degree to which data is useful and applicable to the business purpose for which it is collected.
Reliability	The extent to which data is stable and can be depended upon to produce consistent results over time.

Timeliness	The degree to which data is current and available when required for its intended purpose.
Traceability	The ability to track data throughout its lifecycle, including its origin, transformations, and use.
Validation	The process of confirming that data meets predefined rules, standards, and formats in accordance with defined business, operational, or technical requirements.
Uniqueness	The assurance that each entity is represented only once within a dataset, without duplication.
Data Accountability Framework	A City-wide framework that identifies roles, responsibilities, and accountability for data management activities.
CIMS (Corporate Information Management Services)	The division within the City Clerk's Office responsible for information and data governance leadership.
Structured Data	Data organized according to a predefined schema or format, typically stored in databases, spreadsheets, or other structured repositories, making it easily searchable, reportable, and processable.
Semi-Structured Data	Data that does not conform to a fixed relational structure but contains organizational elements such as tags, metadata, or hierarchical formatting that supports processing and interpretation. Examples include XML, JSON, email messages, and log files.