POLICY		**CAT-SUB-####**	
Data Policy		**Category** GOV - Governance	**Sub-category** COR - Corporate
Approval Type COUNCIL	**Department/Division** Corporate Services/Legislated Services	**Author and Position** Linnea Scian, Project Manager, Data Governance & Quality	
Date Approved Click here to enter a date.	**Last Reviewed/Amended** Click here to enter a date.	**Next Review Date** Click here to enter a date.	

Related Policies or Procedures

- Access and Privacy Policy
- Confidentiality of Information Policy
- Conflict of Interest Policy
- Corporate Accountability and Transparency Policy
- City of Kitchener Open Data Licence
- Information Management Policy
- Municipal Freedom of Information and Protection of Privacy Act
- Public Engagement Policy
- Records Retention By-law
- Responsible Use of Generative Artificial Intelligence (GenAI) Policy

---

Policy Purpose

Data is a corporate asset that the City of Kitchener holds in trust and manages to maximize public value while protecting privacy and security.

This policy establishes city-wide expectations for managing data across its lifecycle (collection, use, storage, protection, sharing, and disposition) to support service delivery, evidence-informed decision-making, transparency, and legislative compliance.

The policy is supported by corporate standards, workflows, and control frameworks maintained by the appropriate corporate authorities.

Definitions

Appendix “A” to this Policy is a glossary of definitions.

Policy Scope

Applies to all City of Kitchener employees, divisions, and departments, and to third parties (consultants, contractors, neighbourhood associations, arms-length organizations, and affiliated groups) that collect, access, store, process, or use City data on behalf of the City. Exceptions may apply where data is governed by external legislation, sovereignty principles, or agreements. Non-compliance may result in disciplinary action, contractual remedies, or legal consequences.

Application

☒ Employees
- All employees

☒ Unions *(Indicate below which categories apply: All Unions, CUPE 68 Civic, CUPE 68 Mechanics, CUPE 791, IATSE, IBEW, KPFFA)*
- All unions

☐ Council

☐ Specified Positions*:* Click or tap here to enter text.

☒ Other: All Third Party Service Providers, volunteers, and any other persons providing programs or services on behalf of the city

Policy Content

The following principles and practices establish the minimum expectations for managing City data as a corporate asset across its lifecycle, including governance, protection, sharing and accountability.

1. Guiding principles

The city manages data according to the following principles:

Data is a corporate asset: City data is managed as a corporate asset across divisions and throughout its lifecycle, with clear stewardship and accountability.

Accessible and usable: Staff should be able to find and use the data they need to deliver services and make decisions, supported by training and consistent practices, while maintaining appropriate access controls.

Open and transparent by default: The City shares data internally and publishes data publicly unless there is a clear legal, privacy, security, contractual, or safety reason not to, including limitations under MFIPPA and licensing.

Safe, secure, and protected: Data is protected using proportionate safeguards, least-privilege access, and recognized control frameworks; privileged access is limited to authorized business needs.

Responsible, equitable, and adaptable: Data is used ethically and in ways that support equitable outcomes, is structured to enable interoperability where feasible, and governance evolves as needs and technology change.

2. Data lifecycle management

The City manages data across its lifecycle. Staff and third parties must follow these minimum expectations:

2.1. Collect

- Collect only the data required to meet a defined business purpose and legal authority.
- Per the Access and Privacy Policy, provide a notice of collection when collecting personal information.

2.2. Use

- Use data only for authorized business purposes and in alignment with the purpose for which it was collected.
- Following internally-managed documentation, apply professional judgment and verify outputs when using automated or algorithm-assisted analysis to inform decisions, including artificial intelligence (AI).

2.3. Store

- Store City data in approved City repositories and systems; do not store City data in unapproved locations.
- Store City data in Canada whenever possible and follow corporate privacy and risk requirements when exceptions are necessary.

2.4. Protect

- Label and protect data using the City's data sensitivity labels and handling requirements.
- Limit access to non-public data to authorized users with a business need and appropriate safeguards.

2.5. Share

- Share data internally and externally only where authorized and with appropriate agreements and safeguards.
- Publish open data where lawful and appropriate under the Open Data Licence and corporate open data practices.

2.6. Retain and dispose

- Manage official records in accordance with the Information Management

Policy and Records Retention By-law.

3. Equity in data use

The City of Kitchener is committed to using data in ways that improve outcomes, increase opportunities for engagement and participation, and reduce barriers for equity-denied groups. Equity considerations must be incorporated when collecting, analyzing, interpreting, storing, and sharing data.

Considerations include:

- Data use must respect privacy, dignity, and legal obligations.
- Data must not be used to further stigmatize or exclude individuals or communities.
- Demographic data collection and use must follow corporate standards and guidance approved by the City and maintained by the appropriate corporate authority.

4. Data protection control framework

The City will maintain a data protection control framework aligned to recognized best practices. Implementation will be managed through corporate standards and monitored using a control register, with summary controls published in Appendix “B” to this Policy.

5. Appropriate use of administrator access

When staff have administrator or privileged access to a system, they must only use administrator access for official city business within the scope of their job responsibilities.

6. Open data

6.1. Commitment and objectives

The City is committed to improving transparency and accountability by providing public access to City data in machine and human-readable formats, where lawful and appropriate.

Open data is seen as a collaborative community undertaking to meet the needs of the community, and to monitor changes within the open government data community.

Through open data, the City supports resident engagement, accountability, and innovation by enabling the public, researchers, and businesses to use City data to create insights, services, and applications.

6.2. Open by default

The City will publish data openly by default unless release is restricted by MFIPPA, security risk, contractual or licensing limitations, confidentiality requirements, or other legal obligations.

Open data publication does not override records retention, privacy, or security obligations.

6.3. Licensing and permitted use

Open datasets are released ‘as is’ under the City of Kitchener’s Open Data Licence.

Following the Government of Canada’s Open Government Licence, the City’s Open Data Licence grants a worldwide, royalty-free, perpetual, non-exclusive licence for lawful use (including commercial use), and sets out exclusions and limitations.

6.4. Publication standards

To be considered open, datasets should be published in accessible, machine-readable formats and include sufficient metadata to support discoverability, understanding, and reuse.

Where feasible, published datasets should be maintained over time with clear versioning or change communication, recognizing that permanence does not supersede retention requirements.

6.5. Prioritization of open data release

The City will prioritize datasets for release based on public value and demand, strategic relevance, readiness, and privacy/security/equity considerations.

Prioritization for publishing open data is complemented by community engagement with individuals, businesses and other public sector organizations.

6.6. Maintenance

If staff determine that an open dataset must be corrected, replaced, or removed, the City will update the Open Data Portal record.

6.7. Dataset requests

The City will maintain a public open data request process with transparent request statuses and will communicate outcomes through the established channel.

Where datasets cannot be released due to licensing restrictions, the City will communicate those constraints transparently through the request process.

6.8. Annual publication planning and accountability

As part of the annual data inventorying process, divisions will identify datasets suitable for publication, confirm stewardship/accountability, and support an annual open data publication plan.

7. Annual data inventorying process

At minimum annually, each division must participate in an annual data inventory process to support internal sharing, open data, risk management, MFIPPA compliance and Personal Information Bank (PIB) updates (see GOV-COR-2023 – Access and Privacy).

This process includes:

- Confirm dataset ownership and stewardship, system of record, sensitivity label, and PIB relevance.
- Identify candidates for open data release and document reasons where release is not possible or not appropriate.
- Identify key risks for escalation and remediation.

8. Data sharing with third parties

Third parties collecting or storing data on behalf of the City must comply with City data protection, privacy, and retention requirements and may be subject to contractual remedies.

9. Roles and responsibilities

As outlined in the data governance manual, roles and responsibilities related to data management are as follows.

Legislated Services: Provides corporate leadership for legislative compliance related to information and privacy (including MFIPPA) and alignment with records and information management requirements (retention, legal holds, authorized disposition). Maintains and publishes the Personal Information Bank (PIB) as required and supports escalation for access and privacy matters.

Legal Services: Provide legal advice related to data protection, privacy, and retention requirements.

Reconciliation, Equity, Diversity & Inclusion: Supports divisional staff in the collection, analysis, interpretation, storage, and sharing of demographic data.

Technology Innovation & Services: Ensures the security, integrity, availability, and appropriate access controls for City technology environments and repositories that store or process City data. Supports security controls, monitoring, and incident response related to City data and systems.

Directors, managers, and supervisors: Ensure data under their area's responsibility is managed in accordance with this policy, including assigning appropriate stewardship and ensuring staff have training and appropriate access to perform their roles. Support the annual data inventory process and timely escalation of risks and incidents.

System owners and administrators: Mana system permissions using least-privilege principles; grant and revoke access based on job responsibilities; and conduct regular permission reviews.

All employees and third parties: Collect, use, store, protect, share, and dispose of City data in accordance with this policy and the City's data protection, privacy, and retention requirements. Immediately escalate suspected privacy breaches, security incidents, or misuse of access privileges using established escalation pathways.

10. Escalation process

Staff must escalate promptly when they become aware of:

- Potential or actual privacy breaches involving personal information, including identifiable demographic data (see Access and Privacy Policy, GOV-COR-2023).
- Security incidents involving restricted data or system compromise.
- Misuse of administrator or privileged access.
- Data quality issues that could materially affect public reporting, safety, service eligibility, enforcement, or Council decision-making.
- Disputes over ownership, classification, disclosure or release decisions.

Escalation pathways are outlined in internal documents maintained by the City.

11. Compliance

Failure to comply with data management best practices may lead to:

- Inadmissibility of data in legal proceedings.
- Insufficient data to support business decisions.
- Regulatory sanctions or penalties.
- Unnecessary costs related to data creation, storage, and management.

Employees are responsible for properly managing and safeguarding the information and resources in their care. To support compliance, procedures and guidance materials will be provided as they are developed.

Individuals who willfully disclose personal information or maintain a personal information bank 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 in accordance with section 48(2) of MFIPPA.

Violations of this policy may result in disciplinary action, up to and including termination, in accordance with the City's policies.

Results of Review

☐ No Edits Required
☐ Housekeeping Edits
☐ Substantial Edits
☐ Repeal/Replace

Policy History

Administrative and Housekeeping Changes

Date	Nature of Change
yyyy-mm-dd	Departmental re-organization/Titling changes/ Standing Committee restructuring.

Substantial Changes

Date	Council/CLT Directive
yyyy-mm-dd	As Per Council/CLT Directive - Report #

Appendix A – Glossary of definitions

Data	Statistical, factual, quantitative or qualitative information that is maintained or produced by or on behalf of a city department.
Dataset	A named collection of related fields, with the collection containing data organized or formatted in a specific or prescribed way, often in tabular form.
Data governance	Overall guiding principles, strategic direction, strategic goals and related policies that govern the management and availability (including security and access) of data at the City of Kitchener. It informs and supports program areas throughout the city in their implementation of data initiatives and their delivery of services and activities.
Data inventory	A fully described record of the data assets maintained by the city. The inventory records basic metadata about a data asset including its name, description, contents, update frequency, use licence, owner, maintainer, privacy considerations, data source, contract end dates and other relevant details.
Data management	The process of collecting, storing, organizing, and maintaining data to ensure its accuracy, accessibility, and security for analysis and decision-making.
Data residency	The physical or geographic location where data is stored and processed.
Data sovereignty	Regardless of where the cloud resources are physically located, when data is stored in a cloud environment, the stored data may be subject to the laws of other countries.
Demographic data	Information recorded in any format about a person related to their personal identity, such as: race; national or ethnic origin; religion; age; marital status; gender; sexual orientation.
Information	Resources or records that are offered for use under the terms of the City of Kitchener's Open Data Licence.
Metadata	Provides information about a dataset to make it intelligible, searchable, accessible and useful for users. Can include controlled vocabularies (examples: department names, division names, date formats, KOF vs Kit OF, etc.).
Metadata record	The digital file that contains the metadata related to a dataset, stored directly in the data file itself, or in an accompanying file.
Official record	A record, regardless of media format, which documents City of Kitchener business functions, activities, decisions, opinions, policies, procedures, legal rights, etc. and upon which the City will rely for proof or evidence of the performance of its functions in the regular course of business. All official records must be retained and disposed of in accordance with the City's Records Retention Schedule and the authorized destruction process.
Open data	Data that is freely available to everyone, without restrictions, and can be used, modified, and shared by anyone for any purpose.
Open Data Licence	A legal instrument that grants permission for anyone to access, reuse, and redistribute data with few or no restrictions. These

	licenses promote wide use, allowing for commercial and non-commercial, modification, and distribution, attribution where feasible; attribution is not required under the City's Open Data Licence.
Personal Information	Information about an identifiable person recorded in any format including race; national or ethnic origin; religion; age; marital status; education; medical, criminal or employment history; financial transactions; identifying number or symbol; address; fingerprints; blood type; name where it appears with other personal information; picture; etc.
Personal Information Bank (PIB)	An index of records that lists the type of personal information we collect from our customers with details of how it is collected and who uses it. Municipalities are required under section 34 of MFIPPA to maintain a publicly available PIB. For greater clarity, this listing does not contain the actual personal information of members of the public.
Records management	The systematic control of official records throughout their lifecycle, ensuring their proper classification, retention, and disposal to meet legal, regulatory, legislative, and organizational requirements.

Appendix B – Data governance and protection controls

The City aligns its data governance and protection practices to Centre for Internet Security (CIS) Controls. The controls below summarize minimum expectations; detailed implementation planning and progress tracking are maintained in an internal control register.

Associated roles and responsibilities outlined in internal documents maintained by the City.

Domain	Control	What it ensures	Review cadence
Inventory and Control of Software Assets	Establish and maintain a software inventory	Maintain an inventory of licensed software/services (purpose, publisher, dates, lifecycle info).	Bi-annually (or more frequently as needed)
Inventory and Control of Software Assets	Ensure authorized software is currently supported	Authorize only supported software; document exceptions with compensating controls and residual risk acceptance.	Ongoing review
Data Protection	Establish and maintain a data management process	Define how data is handled across sensitivity, ownership, retention limits, and disposal requirements.	Annually (or when significant changes occur)
Data Protection	Establish and maintain a data classification scheme	Maintain and periodically update the City-wide data classification scheme (labels).	Annually (or when significant changes occur)
Data Protection	Document data flows	Document key data flows, including service provider data flows, based on the data management process.	Annually (or when significant changes occur)
Access Control Management	Define and maintain role-based access control (RBAC)	Define role-based access rights and perform access reviews on a recurring schedule at minimum annually.	Annually (or more frequently as needed)
Security Awareness and Skills Training	Train workforce on data handling best practices	Train staff to identify and properly store, transfer, archive, and destroy sensitive data.	Corporate training cycle (at minimum annually)
Security Awareness and Skills Training	Train workforce on causes of unintentional data exposure	Train staff on common exposure risks (mis-delivery, lost devices, unintended publishing).	Corporate training cycle

Notes:

a) Controls are reviewed on the cadence above and updated when significant organizational, system, or risk changes occur.

b) Where a control cannot be met (example: required unsupported software), the City documents an exception, compensating controls, and residual risk acceptance.