

Category: Governance

Information Management Administrative Directive

Directive Number: GOV - 210

Approved by: CAO/CLT, January 26, 2023

Administered by: City Clerk's Office, Legislative Services

Effective Date: January 26, 2023

1. Background

At the City of Brampton ("the City"), information is created, received, and used every day. Records and information consist of documentary materials created or received by City Personnel during business and are maintained as evidence of business activities. Records and information may be in many formats such as paper, electronic, audio, etc., but they are all information assets that are important to perform daily business functions. These information assets have business value and demonstrate the City's activities, policies, procedures, operations and decisions.

To sustain the continuing conduct of business, comply with all applicable legislation and ensure accountability, the City integrates information management into all its business processes and corporate planning activities.

2. Purpose

The purpose of this Administrative Directive is to establish a comprehensive Information Management program that provides direction on the creation, identification, maintenance, retention, disposal and safekeeping of information under the control of the City of Brampton.

The Information Management program will enable the City to:

- Identify roles, responsibilities, policies, and procedures as required to safeguard information reliability and integrity for the purpose of sound business decisions.

- Meet legislative requirements under the [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#).
- Provide evidence of business activity.
- Meet operational requirements.
- Protect the legal, historical and financial interest of the City, its employees and the public.
- Support the Information and Data Governance Strategy and Framework.

3. Application and Scope

This Administrative Directive applies to all information, in all media and formats, created or received by City Personnel (including elected officials, employees, volunteers of the City, as well as contractors and vendors retained to provide services to the City), in the course of performing their duties.

3.1 Exceptions

Political records of Councillors.

4. Outcomes

- Ensure that all City employees are aware of their responsibilities as they relate to managing information assets under their control.

5. Principles

5.1 Accountability - City staff are stewards of City information assets and are ultimately accountable to the public. Roles, responsibilities, policies and procedures should be established within each department to be in line with this Administrative Directive in order to safeguard the information assets we manage at the City. The City must meet the legislative requirements set out in the [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#). The legal, historical and financial interests of the City, its employees and the public must be protected.

5.2 Compliance - Compliance with this Administrative Directive will ensure that all information created at the City is reliable and retains its integrity throughout its lifecycle.

6. Mandatory Requirements

6.1 Accountability & Integrity

Information must be managed throughout its lifecycle by assigning accountability for the effective and efficient use of information to specialist groups and to the user community. Information must be reliable and accurate, and must be a true representation of the actual event or task. Records must not be altered or tampered with in any way.

6.2 Protection & Availability

City policies and practices provide the means for the City to meet its legal, regulatory and contractual requirements regarding the protection of information assets at the City. In addition, the City must maintain accurate records and information and ensure that they are available and can be retrieved in a timely and efficient manner by City Personnel requiring it for the City's business purposes. The City must collect and use information about people with whom it works with and provides services for. The City of Brampton's [Privacy Administrative Directive](#) and [Privacy Statement](#) support the collection, use, retention, disposal and disclosure of personal information, regardless of whether the information is held in hard copy or digital/electronic form.

6.3 Compliance

The City's Information Management program must comply with all applicable legislation, standards, authorities, as well as, all City policies and practices. Records and information created must accurately demonstrate the City's business activities and decisions, and must be retained and maintained as prescribed by law.

6.4. Retention & Disposition

The City's [Records Retention By-law](#) provides directions on which records and/or information to retain and for what length of time. The length of time a record must be kept and be accessible is based on the legal, regulatory, fiscal, historical and business operational requirements of the City.

Records and information must be securely disposed of immediately following the expiry of their retention periods to mitigate the risk of unauthorized or unnecessary

access. The City's [Records Retention By-law](#) provides directions on how to dispose of records/information that no longer has any business value.

6.5. Openness & Transparency

The public has the right to access information under the control of the City in accordance with the [Municipal Freedom of Information and Protection of Privacy Act](#). Employees and the public also have the right to access and have any errors corrected in their personal information which the City has in its custody or under its control.

6.6. Quality Assurance

The City is required to establish and maintain procedures for information quality assurance and the effective management of records. The City will undertake routine assessments of its information quality and records management processes. The City will promote information quality by means of its policies, procedures and training and awareness initiatives.

6.7. Records and Information Management

Records and Information Management refers to the handling of information assets throughout their lifecycle: from the time they are created/received, while they are used and maintained, until their final disposition (preservation or destruction). The three stages in the lifecycle of a record are:

6.7.1 Creation (Receipt)

The City creates or receives records that document its business activities, functions, policies and decisions. Information should be documented immediately or as close to the time when the event pertaining to it occurred, to make sure all details are captured accurately and appropriately.

Records must be created in all instances when there is a need to be accountable for and/or provide evidence of decisions made and/or actions proposed or taken. Records must be accurate, authentic, reliable and complete.

6.7.2 Use and Maintenance

Records must be maintained in such a way as to make them accessible to others who require use of the information in the record and must be protected against unauthorized access, disclosure or destruction.

There are three basic steps to managing the City's records and information:

- Identify records that document Brampton's business activities.
- Capture and maintain records in approved information management systems.
- Retain records according to the City's [Records Retention By-law](#) and in keeping with any [Municipal Freedom of Information and Protection of Privacy Act](#) and [Municipal Act](#) requirements and/or Legal Holds.

Records and information requiring permanent retention (e.g., Council minutes) must be maintained in an accessible format.

6.7.3 Disposition

This final stage in the lifecycle of a record occurs when records are no longer of any business value and have reached the end of their prescribed retention periods. They are to be routinely disposed of in accordance with the City's [Records Retention By-law](#), to prevent the risk of unauthorized access and use.

Disposition of records and information can occur in one of two ways:

Destruction – Records are destroyed making the information permanently unrecoverable or unreadable. The most appropriate method for destroying records depends upon the records format.

Archive – Records are transferred to Peel Art Gallery Museum and Archives with instructions to preserve information of historical or cultural value contained in the record.

6.8 Information Management Systems

The City's [Records Retention By-law](#) provides the foundation for organizing City records, based on their business functions and activities. This allows for the

consistent application of retention and disposition requirements.

When information is created or received, it must be captured and maintained in an approved information management system to provide authorized access, and to safeguard the City's information assets. Emails and their attachments may also be considered information assets if they are made or received in connection with City business. The information management system used may be for electronic or tangible copy records.

Not all information created or received by the City needs to be maintained as an official record. Transitory records can be destroyed or deleted in a timely and effective manner when they no longer have any business value. The Records Decision Tree (see Appendix) provides guidance on how to differentiate between information that is official or transitory. Personal documents may be retained or destroyed by the individual whenever they choose.

In order for individuals to access and use corporate records, such records must be identified using appropriate metadata to describe the structure, content, and context. The metadata attached to the record allows for quick and easy access by authorized individuals. This information includes: title of record; description; creator; and retention time frames and disposition actions. This will allow for the proper classification of the record.

City business must be performed on official City information management systems. Employees using instant messaging or other transient technologies for official business must manage corporate messages as official records. The use of social media tools (Facebook, Twitter, etc.), for conducting City business may be limited to activities permitted by and in accordance with the City's policies and procedures. All official digital records (e.g.: email, spreadsheets, presentations, data, images, videos etc.) must be captured and maintained in approved digital information management systems such as SharePoint and PeopleSoft. All paper records must be properly filed and maintained in a secure cabinet or locked drawer.

Orphaned information assets are managed by the Information Management Team. These need to be managed appropriately throughout their lifecycle to ensure compliance with the Records Retention Bylaw. The BRIMS_ADMIN security group (Information Analyst) must be provided with ownership and access to manage the lifecycle of the information.

7. Roles and Responsibilities

7.1. Chief Administrative Officer

- Establishes the corporate vision, values and strategies that address information as a strategic business asset of the City.
- Ensures the establishment of an effective information management program within the City.
- Ensures employees are aware of their obligation to manage information appropriately.
- Ensures all data protection and security of information policies and procedures are understood, implemented, and adhered to.
- Ensures the day-to-day practice and enforcement of the processes outlined in this Administrative Directive.

7.2. City Clerk

- Ultimate authority for the City's information management practices and programs.
- Oversees this Administrative Directive including (but not restricted to): compliance, coordination of implementation activities, and monitoring results.
- Accountable for the compliance with the [Municipal Act](#) and the [Municipal Freedom of Information and Protection of Privacy Act](#), as they address records and information management.
- Provides on-going support on day-to-day activities including privacy impact assessments, incident management and access requests.

7.3. Chief Information Officer (CIO)

- Resources an information security program that assesses and manages information risks in the enterprise network.
- Investigates any access or security breach including the loss, inappropriate access or unauthorized disclosure of the City's electronic records and information.
- Ensures that retention, disposition, access, and security are an integral part of each stage in the system development lifecycle.
- Safeguards the availability of electronic information through appropriate data backup and recovery practices.

7.4. Deputy City Clerk

- Business owner of Electronic Document and Records Management System.
- Provides leadership, direction, and vision for the City's overall Information Management program.
- Provides authority for Information Management processes, procedures, and methodologies and for approving contractors for Information Management services (digitization, shredding and storage).

7.5. Manager, Information Governance

- Raises awareness of Information Management and promotes compliance with this Policy and all related practices and guidelines through training and awareness initiatives.
- Oversees the creation of tools, policies, standards, and guidelines related to Information Management.
- Work with Information Technology to obtain and develop software that enables Information Management.
- Provides advice and support to all business areas on information management processes and requirements.
- Measures and reports on the overall quality and health of the Information Management program and systems.
- Administrative access to all City information management systems to conduct periodic reviews of the systems and their contents as well as ensure compliance with Policies and By-laws.
- Administrative access to all City information management systems to provide program-specific support.
- Manages the lifecycle of orphaned information assets in compliance with the Records Retention By-Law, using the BRIMS_ADMIN security group.

7.6. Department Heads

- Ensures their business processes comply with this Administrative Directive and current information management best practices.
- Ensures that employees are aware of and follow the Information Management Administrative Directive and practices as they apply to their process, including the timely creation of records as well as timely destruction authorization sign-off.
- Ensures a delegate is named as the Information Management Coordinator/Information and Data Steward, and encourages their full participation in the Information Management program.

7.7. Information Management Coordinators

- Uses the information, guidance and tools found on the internal Records and Information Management Website to assist in proper information management within the City.
- Actively participates in training and awareness events hosted by the Information Management Team.
- Communicates and trains team members on the proper use of information management systems and general handling of records.
- Monitors business area's compliance with this Administrative Directive.
- Monitors business area's access permission to electronic information management systems.

7.8. All City Employees

- Ensures familiarity with this Administrative Directive and City information management practices.
- Creates accurate and reliable information to support business activities.
- Protects personal and confidential information throughout its lifecycle.
- Ensures records are stored in a City approved information management system.
- Retains and disposes of records according to the City's [Records Retention By-law](#).
- Ensures appropriate protection against unauthorized use, loss/theft of records, and should a breach occur, promptly notify the City's Privacy Officer.

8. Monitoring and Compliance

- 8.1 The Records and Information Management office produce a variety of reports to monitor compliance with information management rules. These reports are sent to staff on occasion to aid the correction of any errors.

Periodic reviews of systems and repositories occur to ensure that those records are being managed in accordance with the [Records Retention By-law](#).

8.2. Consequences of non-compliance

If information assets are not managed correctly it could result in a risk to the City. Failure to follow this Administrative Directive may result in:

- Breach of confidential or personal information
- Inability to comply with legal requirements as outlined in the [Records Retention By-law](#)
- Loss of vital information
- Unable to identify historical, vital, or business critical records
- Unclassified or misclassified information that could be disposed of prematurely
- Inability to find information due to poor controls

9. Definitions

- 9.1. **Archives** – refers to records that are considered to have enduring value and must be transferred to Peel Art Gallery Museum and Archives for permanent or long-term preservation.
- 9.2. **Business Value** – refers to the concept that records, as information assets, have value. This is measured by the length of time the record is kept before being disposed or destroyed.
- 9.3. **Corporate Records** – are official records documenting the City of Brampton’s business transactions, decisions and activities.
- 9.4. **Information Assets** – Information assets are bodies of information, defined and managed as a single unit so they can be understood, shared, protected, and used efficiently. Information assets have recognizable and manageable value, risk, content and lifecycles.

- 9.5. Information and Data Governance Strategy and Framework** – the process of managing the availability, usability, integrity and security of information and data stored in City systems, based on internal standards, policies, controls, and governance best practices.
- 9.6. Information Management System** – a system (manual or electronic) that captures, controls and provides access to records over time.
- 9.7. Internal Records Management Website** – accessed via the City’s Service Catalogue, this one-stop shop for internal services includes the Records and Information Management page hosting useful resources, to help staff manage their information assets.
- 9.8. Legal Hold** - refers to a hold order or notice received by the City, which requires the City to preserve all forms of relevant information, as a result of reasonably anticipated investigations, access requests, audit or lawsuit. A legal hold suspends the normal disposition or processing of records.
- 9.9. Metadata** – is data describing context, content and structure of records and their management over time. For example, an image may have metadata that describes how large the picture is, when it was created and by whom, the image resolution and other data. Or, a file folder containing paper documents may be labelled with a title describing the subject matter, a unique reference number and a date.
- 9.10. Official Records** – are any records or information that document the official actions, decisions, policies, or procedures at the City of Brampton.
- 9.11. Orphaned Information Assets** - can be physical or electronic and do not have a defined owner. This can result from corporate reorganization, termination of employment, or other scenarios resulting in termination of active ownership.
- 9.12. Personal Documents** – are documents that are not related to City business and do not have to be kept in an approved information management system (e.g.: personal communications, invitations). They may be retained or destroyed by the individual whenever they choose; however, where personal documents are part of an investigation or litigation, they must be maintained and provided to the requestor.

9.13. Political Records - Political records document a Councillor's relationship with their constituents and are considered personal property of the Councillor.

9.14. Records and Information – any recorded information, regardless of media type or format, which documents the City of Brampton's business transactions, decisions, and activities.

9.15. Records Decision Tree - provides guidance on how to differentiate between records that are official and records that are transitory.

9.16. Transitory Records – are records that may be used in the conduct of City business but are of short-term value and do not have to be kept in an approved information management system. They may be routinely destroyed when they are no longer required.

10. References and Resources

This Administrative Directive should be read and applied in conjunction with the following references and resources as updated from time to time. Please note that some of the following documents may not be publicly available.

External references

- [Municipal Freedom of Information and Protection of Privacy Act](#)
- [Municipal Act](#)

References to related bylaws, Council policies, and administrative directives

- [Accountability and Transparency](#)
- [Records Retention By-law](#)
- [Use of Information Technology Resources](#)
- [Privacy Administrative Directive](#)

References to related corporate-wide procedures, forms, and resources

- [Privacy Statement](#)
- [Digitization SOP](#)

Revision History

Date	Description
2016/10/06	Replaces Records Management Policy 14.8.0 approved in 2003.
2023/01/26	Approved by CAO/CLT. Replaces Information Management policy 14.8.1
2026/01/26	Next Scheduled Review (<i>typically three years after approval</i>)

APPENDIX

City of Brampton Records Decision Tree

