

Information Management Guideline – Managing Information in Collaboration Tools

Guideline No.: CIMS-G020

Version No.: 1.0

Issued On: December 8, 2023

Issued By: Corporate Information Management Services, City Clerk's Office

Subject: Collaboration

Keywords: Collaboration, Records Management

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 the standardization of Information Management in the City of Toronto.

Acknowledgements: This Guideline acknowledges the efforts, subject matter expertise, and oversight provided by the following:

- **Project Sponsor:** Kristie Pratt, Deputy City Clerk, Corporate Information Management Services
- **Divisions & Business Units:** Corporate Information Management Services, Technology Services Division, Office of the Chief Information Security Officer

Contact Information:

Kristie Pratt

Deputy City Clerk

Corporate Information Management Services, City Clerk's Office

City Hall, 13th floor, West Tower

100 Queen Street West

Toronto ON M5H 2N2

Tel: (416)392-9673

Kristie.Pratt@toronto.ca

Contents

Information Management Guideline – Managing Information in Collaboration

Tools	1
1. Introduction	4
2. Purpose	5
3. Application	5
4. Guideline: Managing City Information in Collaboration Tools	6
4.1 Storing and Managing Information in Collaboration Tools	6
Appropriate City Record Keeping Repositories	6
Maintenance and Storage of Instant and Workspace Messages	7
Migration of Records to Appropriate Recordkeeping Repositories	7
Maintenance and Storage of Images	7
4.2 Documenting Information and Decisions in Collaboration Tools	8
Document Meeting, Instant Messaging, and Workspace Decisions	8
4.3 Organizing Information in Collaboration Tools	9
4.4 Applying Access Controls in Collaboration Tools	9
4.5 Internal and External Sharing in Collaboration Tools	10
Defining Ownership in Shared Collaboration Tools	11
Externally Managed Collaboration Applications	12
4.6 Deleting and Dispositioning Information in Collaboration Tools	12
Deletion of Transitory Information	12
Disposition of Information	12
5. Roles and Responsibilities in Managing Collaboration Tools	13
Assigning Workspace Administrators	13
5.1 City Clerk's Office will:	13
5.2 Division Heads will:	14
5.3 Workspace Administrators will:	14
5.4 All Employees will:	15
5.5 Chief Technology Officer (Technology Services Division) will:	15
7. References	16
8. Contact	16

9. Guideline Approval	17
10. Guideline Review	17
Appendix	17
Appendix A: Definitions	17

1. Introduction

The City of Toronto is dedicated to modernizing and transforming its services and embracing new approaches to work. The COVID-19 pandemic, remote work, and City office modernization have cemented collaboration software and applications as necessary tools in daily operations. From meeting and messaging applications to document sharing and project management tools, City staff use several collaboration tools daily.

Collaboration tools are applications or software features that support business activities between colleagues, such as writing documents, having discussions, tracking project performance or issue tickets, sharing files, or brainstorming. An application can be considered a collaboration tool when it is used simultaneously by multiple employees working together. Collaboration software features include, but are not limited to:

- Co-editing documents from a shared location;
- Presentations, screen sharing, and recording videos;
- Exchanging chat messages;
- Project or ticket tracking;
- White boarding; and
- File sharing.

Authorized tools with collaboration features in use by the City include, but are not limited to:

- Microsoft Office 365 (MS Teams, SharePoint, OneDrive, Skype, OneNote, etc.)
- Atlassian solutions (JIRA, Confluence, etc.)
- WebEx
- Cisco Jabber
- Salesforce
- SAP
- CheckMarket Survey Tool
- ServiceNow
- ELI
- T-Recs

While standalone chats, messages and content produced within collaboration tools often contain [transitory information](#) that does not need to be kept or managed, there are situations where business decisions are made within collaboration tools—in which case City staff have an obligation to manage and protect City information through its lifecycle and meet recordkeeping obligations.

2. Purpose

The purpose of this guideline is to provide a framework, advice, and an overview of the Information Management responsibilities for City staff when using collaboration tools and the requirement to document City decisions.

This guideline contributes to the City's [Information Management Accountability Policy](#) and [Corporate Strategic Plan](#) by bolstering its commitment to build trust and confidence in local government, ensuring *A Well-Run City*, which includes the management of City records and information to:

- Support new approaches to work and enable high quality, resilient and innovative public services;
- Support the use of data and evidence to inform decision-making; and
- Ensure an accountable and transparent municipal government.

This guideline will aid City staff in balancing their need to use collaboration tools to innovate and modernize their lines of business with their responsibility to document decisions and manage information in accordance with the [Municipal Freedom of Information and Protection of Privacy Act](#) (MFIPPA), [Toronto Municipal Code Chapter 217](#) (Chapter 217), [Information Management Accountability Policy](#) (IMAP), [Acceptable Use Policy](#) (AUP), [Digital Infrastructure Strategic Framework](#) (DISF), [Protection of Privacy Policy](#), [Digital Image Management Policy](#), and [Electronic Records Disposition Guideline](#).

3. Application

This guideline applies to all City of Toronto Divisions and employees, volunteers, and third parties who access, create, store, and use records, data, and information on behalf of the City.

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

This guideline only applies to authorized collaboration tools that are accessed or used within City technology assets in accordance with the AUP. Staff are encouraged not to use system, service, hardware, and network assets not owned, supplied, or leased by the City for the performance of their duties and responsibilities, including collaboration.

4. Guideline: Managing City Information in Collaboration Tools

4.1 Storing and Managing Information in Collaboration Tools

Appropriate City Record Keeping Repositories

While collaboration tools are good for facilitating brainstorming, white boarding, quick-messaging and co-editing drafts, they are inappropriate recordkeeping repositories due to their limited control over records and the potential for alteration or loss of records or decisions over time. Any business decisions or actions created or recorded in collaboration tools must be routinely moved to appropriate City recordkeeping repositories, such as:

- Shared Network Drives
- Toronto Records OpenText Repository (T-Recs)
- SharePoint
- Line of business applications
- Image Library

Risks of leaving City information or business decisions within collaboration tools not designed for records storage include:

- **Restricted access:** Limited access to the collaboration tool may mean employees who need access do not have it. Additionally, access is lost over time as projects and staff move on or retire.
- **Difficulty finding records:** Records may not be named, classified or filed appropriately and may be missed when responding to Freedom of Information (FOI) requests or for a legal holds or searches.
- **Incomplete records:** The integrity, authenticity, usability, and trustworthiness of records are not maintained because the records are dispersed.
- **Unauthorized destruction:** Records may be inadvertently destroyed due to non-existent, ambiguous or inconsistent records management procedures. Collaboration tools may also be configured to auto-delete content, resulting in unauthorised deletion.
- **Inappropriate access:** Leaving records in the tool beyond their active use may mean sensitive or confidential information is accidentally disclosed as user access to the tool changes.

Before looking to download or use any new collaboration tool, please consult Corporate Information Management Services (cisp-consults@toronto.ca) and your [Business Relationship Manager](#) (BRM) at Technology Services Division (TSD) to ensure the tool is an authorized collaboration tool and safe to use.

Maintenance and Storage of Instant and Workspace Messages

Collaboration tools can facilitate instant messaging one-on-one, in group chats, and in workspaces for entire groups or teams (e.g., WebEx Space). Instant or workspace messaging may produce business decisions, or records, that require proper documentation, retention and lifecycle management.

Most messaging systems that facilitate instant messaging are configured so that messages are automatically deleted from the system within a limited amount of time (e.g., purged after 30 days). Unlike instant messages, conversations within a workspace are often retained until the messages are manually deleted or the workspace is decommissioned. While collaboration tools and instant messaging applications may have repository functionalities and even have areas to save files, they are not considered appropriate recordkeeping repositories, and you must:

- Ensure each space has a clear Workspace Administrator responsible for managing the workspace;
- Document any conversations, collaboration or white boarding that provides evidence of a decision or work activity;
- Copy, summarize, or transcribe the conversation information to another document;
- File conversation transcriptions and collaboration documents in an appropriate recordkeeping repository; and
- Capture record keeping metadata.

Messages may record or produce decisions that are relevant to an FOI search or legal hold.

Migration of Records to Appropriate Recordkeeping Repositories

Digital migration refers to the process of moving records, including their existing characteristics, from one hardware or software configuration to another. Migrate, summarize, or transcribe information that provides evidence of a decision from any collaboration tool to an appropriate recordkeeping repository on a regular basis or when projects or correspondence are completed. Other migration considerations include:

- Capture what information, including metadata, must be migrated to a recordkeeping repository;
- Document who is responsible for regularly ensuring records are migrated;
- Test what was migrated to ensure the migration is complete and unaltered;
- Confirm that the records remain accessible to appropriate users; and
- After successful migration, delete source information from the collaboration tool.

Maintenance and Storage of Images

Image-based records require specialised management to streamline access, support business requirements, and reduce the risks associated with privacy and copyright. The

City Clerk's Office offers an Image Library Service as a modern digital solution to help you streamline your image management, sharing, and workflow needs. Contact imagelibrary@toronto.ca to find out more, request a consult or receive training.

4.2 Documenting Information and Decisions in Collaboration Tools

All City staff are responsible for [documenting their actions and decisions to adhere to their legislated obligations](#). City staff must create full, accurate, and complete records of all service delivery activities, regardless of how they were communicated.

To comply with duty to document requirements established within the City's Information Management Accountability Policy and [Municipal Code Chapter 217, Records, Corporate \(City\)](#), City staff must:

- Ensure an [appropriate recordkeeping repository](#) is in place for creating and maintaining City information; and
- Create and maintain adequate records of their decisions

For more information on what constitutes an appropriate recordkeeping repository, and documenting business decisions, please contact CIMS (cisp-consults@toronto.ca).

Document Meeting, Instant Messaging, and Workspace Decisions

Document meetings, instant messages, and workspace messages conducted or created using collaboration tools (e.g., WebEx). This may be a simple meeting minutes text file or an audio or audiovisual recording.

The decision to record a call or meeting is at the discretion of the organizer. If recording a meeting, meeting organizers should inform all participants and presenters prior to the start of the meeting. If a meeting is not recorded, and a business decision is made during it, please capture that decision per the previous section.

Meeting Recordings with the Public and Notice of Collections

When recording a call or meeting with a member of the public, personal information may be collected. Therefore, before using a collaboration tool to record a call or meeting with any member of the public, the meeting organizer must ensure City privacy protection requirements are identified. Specifically, the meeting organizer must consult with the City's Information Collection unit (forms@toronto.ca) who will help determine those requirements, including whether a *Notice of Collection* must be provided before a meeting.

Providing a Notice of Collection statement:

- Confirms to an individual that the City has the legal authority to collect their personal information;
- Recognizes a person's right to know and understand the purpose for the collection of their information;

- Allows the person to make an informed decision as to whether or not to provide the information; and
- Provides a person with direct contact information should they have a question about the collection at any time.

For more information on Information Collection requirements, including [Notice of Collection statements](#) and whether your meetings will require them, please contact the Information Collection unit of CIMS (forms@toronto.ca).

4.3 Organizing Information in Collaboration Tools

Follow information and records management best practices when using collaboration tools, regardless of their communication and documentation features.

Use your Division or Section's established file plans and naming conventions to name folders and files created in collaboration tools; please contact CIMS and review the City's [File Planning 101 Guideline](#) for help in developing File Plans.

Collaboration tools that do not use hierarchical folder structures will benefit from the application of consistent controlled terminology and descriptive metadata standards that meet your team's business needs and are aligned with City standards and best practices.

Always use a standard file naming format that includes metadata elements like a clear description of the document, the version number, the protection classification and the date of approval as outlined within the City's [Information Protection Classification Standard](#), [Descriptive Metadata Standard](#) and [Records Management Metadata Standard](#). Where possible, configure collaboration tools to automatically capture required metadata.

It is recommended to identify all information documenting business decisions that needs to be moved to an appropriate recordkeeping repository, either on a routine basis or at the conclusion of a project.

4.4 Applying Access Controls in Collaboration Tools

Collaboration applications may collect and retain personal or sensitive information. It is City Staff's responsibility to protect the confidentiality, integrity, and availability of that information by ensuring only authorized users can access it. Within collaboration tools, access controls and processes should be in place and effective practices should be followed to adequately protect the City from security threats and breaches. Access controls are essential in managing user identities and related access permission within a collaboration tool.

While enterprise application, system and repository access controls are often administered through Technology Services Division (TSD) in accordance with City

policy and best practices, collaboration tools often allow for Divisional authorized users and Workspace Administrator to create and manage access controls within workspaces.

Below are key access control considerations and requirements for collaboration applications and their workspaces:

- Requesting Access
 - There is a user registration process
 - The reason for requesting access is consistent with job responsibilities and authorized work
- Approving Access
 - Access requests are approved by appropriate Supervisor/Manager
 - Records of access approvals are maintained
- Providing Rights
 - Restrict access by using and configuring predefined role permissions
 - Access rights based on need-to-know and principle of least privilege
- Monitoring Access
 - Promptly review access when an employee changes responsibilities
 - Review access for employees on extended absence or transfer assignment
- Removing Access
 - Remove access for employees who no longer have a business need to access
 - Revocation of authentication credentials follows a formal process

All collaboration tools and related access controls and processes must align with the City's [Access Management Policy](#), [Access Control Standard](#) and [Mobile Device Management Policy](#). For more information, please contact the Office of the Chief Information Security Officer (CISO) (CISO@toronto.ca) or [Technology Services Division](#).

4.5 Internal and External Sharing in Collaboration Tools

External sharing is the practice of providing people and organizations with access to City information, records, and data they cannot access through existing processes, data systems or technologies. Internal sharing is the practice of exchanging Divisional information, business records or data with other City Divisions, or Sections, that is not routinely shared through existing systems, technologies, or practices.

Many collaboration tools have sharing features and give authorized users or Workspace Administrators a large degree of control over how they access and share information. While internal and external sharing is beneficial, it inherently carries privacy and security risks to City records and technology infrastructure.

In the City's context, there are five primary forms of internal and external sharing:

Internal Sharing

- **Intra-Divisional sharing** – information exchange between business units belonging to the same City Division
- **Inter-Divisional sharing** – information exchange between two or more City Divisions

External Sharing

- **Inter-governmental sharing** – information exchange between a City Division and another government organization, such as an agency, board, commission, municipality, provincial government, or the federal government
- **Research sharing** – information exchange between a City Division and an academic, community or public research organization, such as a university, or hospital.
- **Business-to-business sharing** – information exchange between a City Division and a third-party vendor, service provider, or contractor

Before enabling or allowing for internal or external sharing within a collaboration tool or a workspace, the sensitivity of the information within the tool must be considered and defined, access controls must be defined and enabled and CIMS must be consulted (cisp-consults@toronto.ca).

Defining Ownership in Shared Collaboration Tools

Defining ownership of a collaboration space and its records is a key requirement when creating, or participating in, a collaboration tool with another Section, Division or external partner.

For intra-Divisional and inter-Divisional collaboration spaces, CIMS recommends clearly defining one Division, Section or Unit as the owner of the space and its records. The owner will be responsible for [assigning a Workspace Administrator](#), [managing the authoritative records produced within the space](#) and [dispositioning records](#).

Non-owner Divisions, Sections or Units participating in the space are not responsible for maintaining the authoritative records and may keep reference copies to be treated as transitory records, so long as any record produced via collaboration methods has been retained appropriately by the owner.

For inter-governmental, research and business-to-business sharing, ownership should be defined through appropriate agreements including but not limited to a Contract, Information Sharing Agreement, Memorandum of Understanding, Memorandum of Agreement, Terms of Use, Research Agreement, or a Common or Integrated Program Agreement. Divisions must contact their [divisional Legal Services representative](#) to advise on information sharing related agreements, and to assist in developing the terms and conditions of an agreement. Additionally, contact CIMS (cisp-consults@toronto.ca)

to assist in determining specific requirements regarding records retention, use and disposition, privacy protection, notices of collection, and/or metadata.

Externally Managed Collaboration Applications

When using a collaboration application hosted by an external vendor or partner, the advice provided in this document regarding establishing a Workspace Administrator, duty to document, records migration and storage, and access controls apply. Please contact the Office of the CISO (CISO@toronto.ca) and CIMS (cisp-consults@toronto.ca) before using collaboration tools managed by external partners.

4.6 Deleting and Dispositioning Information in Collaboration Tools

While often used interchangeably deletion and disposition are different actions. Deletion is the obliteration or destruction of specific information and is a mechanism for disposition. Disposition is a formal process and represents the end of the records life cycle. Records may be either deleted or retained permanently as defined by the applicable retention schedule. The disposition of records must be done in such a way to comply with City best practices and legislation and is approved by Division Heads or their designate. For example, files are approved for deletion after the disposition approval process.

Deletion of Transitory Information

Consistent and vigilant identification and deletion of [transitory information](#) in collaboration tools is vital and recommended for completion on a routine schedule. CIMS provides consultation to support configuration to administer timely and consistent deletion of transitory information in collaboration applications.

When records have been successfully migrated to an appropriate recordkeeping repository and are no longer needed on a collaboration tool, the documents become redundant and can be manually deleted or left for deletion within tools that have automated and timed deletions.

Disposition of Information

Disposition of information must be done in accordance with applicable policies, laws and by-laws, including Chapter 217 of the Municipal Code, the City's records retention schedule, and the [Information Management Guideline - Electronic Records Disposition \(toronto.ca\)](#).

It is recommended to disposition records within appropriate recordkeeping repositories that have been created to facilitate disposition. Recordkeeping repositories are enabled with approval workflows, audit trails and other features that ensure the disposition process is properly facilitated in accordance with City best practices and legislation.

Therefore, it is recommended that all records be migrated from collaboration tools to appropriate repositories in a timely manner; retained in those repositories in accordance with the City's [records retention schedule](#) and dispositioned within those repositories.

For more information about the disposition process please review the City's Electronic Disposition Guideline. You may also contact CIMS (cisp-consults@toronto.ca).

5. Roles and Responsibilities in Managing Collaboration Tools

Assigning Workspace Administrators

Many tools require Divisional collaboration *workspaces* to be created. Some of these workspaces require monitoring; managing access permissions; and/or periodic migration of information. Each workspace will also have its own configuration options, search interfaces, and means of migrating information to an appropriate recordkeeping repository.

For each collaboration tool workspace and/or authorized user group onboarding to a collaboration tool, an application *Workspace Administrator* role must be defined and assigned, and might be a team leader, project owner, Application Owner, manager and/or records management resource as part of their regular duties. They are responsible for configuring and maintaining the workspace as well as achieving and maintaining appropriate protection of the information within the tool, which includes records management, security, and privacy protection responsibilities.

A Workspace Administrator must not be confused with an *Application Administrator*. An Application Administrator has elevated permissions and is responsible for the overall enterprise maintenance of an application including processes and methodologies for maintaining, enhancing and managing the application. Roles and Responsibilities

5.1 City Clerk's Office will:

- Lead the development and implementation of City policies, standards, guidelines, best practices and procedures to promote data governance and the proper maintenance, retention and deletion of information;
- Lead the development and implementation of City policies, standards, guidelines, best practices and procedures to promote the management and protection of personal information and management of and access to City information within collaboration tools;
- Consult with Divisions regarding new and current collaboration tools, their functions and fit with Divisional and information management requirements;
- Provide consultation in the development of file plans, records migration, retention and disposition processes, access permissions and information protection classifications to ensure compliance with legislation and City policy, namely the IMAP, the Electronic Disposition Guideline, the Information Protection Classification Standard, the File Planning Guideline and the Protection of Privacy Policy;
- Review Divisional practices for the collection, use, disclosure, and authorized disposition of information within collaboration applications;

- Provide training and education that increases awareness and knowledge of privacy and information management, records lifecycle management and disposition requirements; and
- Develop and promote the adoption, management and use of appropriate metadata, controlled vocabularies and data classifications.

5.2 Division Heads will:

- Ensure alignment with this guideline and related technology administration procedures and requirements within their Division;
- Consult with TSD BRM, CIMS and appropriate technology gating boards when acquiring or onboarding onto a new collaboration tool, to ensure that it meets government recordkeeping needs outlined in MFIPPA, IMAP and Chapter 217;
- Ensure collaboration tools used by staff follow the City's Acceptable Use Policy;
- Ensure appropriate staff are assigned as Workspace Administrators of collaboration tools or associated spaces;
- Ensure authorized users are properly trained to increase their awareness and knowledge about information management within collaboration tools;
- Ensure Workspace Administrators of the tool are properly trained in technical capabilities as well as information management responsibilities surrounding security including access controls, protection of privacy, records management and data governance;
- Ensure Division has an established and defined preferred recordkeeping repository, or repositories, that are meant to manage and maintain Division's records;
- Ensure all employees have access to, and are aware of, the Division's preferred record keeping systems to manage and retain records;
- Ensure information and its metadata within Divisional collaboration tools are managed throughout their lifecycle in accordance with the applicable retention schedules, from creation or collection to migration and disposition in an appropriate recordkeeping repository; and
- Ensures staff are aware of [Breach Management guidelines](#) and procedures.

5.3 Workspace Administrators will:

- Understand the business purpose of the collaboration tool and ensure it is used appropriately by authorized users and guests;
- Oversee, assign, and manage appropriate collaboration tool workspace's permissions and access;
- Where retention and disposition is enabled within a collaboration tool, consult with CIMS to ensure appropriate [records retention classifications](#) are applied to records and ensure disposition takes place in accordance with the [Electronic Records Disposition Policy](#);

- Where retention and disposition is not enabled within a collaboration tool, lead the movement of records on a regular basis or when projects or communications are completed to an appropriate recordkeeping repository;
- Consult with CIMS and lead file planning activities on behalf of business, including establishing folder structures or custom metadata;
- Make information in a collaboration tool workspace available in response to [FOI](#) requests;
- Restrict access to information, in accordance with the appropriate [information protection classification](#), to those individuals who require it in order to perform their duties;
- Document how your team has configured and organized the collaboration tool's workspace to ensure the information can be maintained and migrated; and
- When a collaboration tool workspace is used inter-Divisionally, cross-Divisionally or across jurisdictions, identify a lead body to be responsible for the collaboration tool's records.

5.4 All Employees will:

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

5.5 Chief Technology Officer (Technology Services Division) will:

- Integrate information and records management, privacy and access requirements by design into collaboration tools and their implementation activities

in accordance with the requirements of Municipal Code Chapter 217, Corporate Records and MFIPPA, in both operational and capital projects;

- Develop and maintain related collaboration tool policies, standards, procedures and architectures; and
- Where appropriate, develop and administer collaboration tool training for authorized users and Workspace Administrators.

7. References

- City of Toronto, City Clerk's Office. (2009). [Descriptive Metadata Standard](#)
- City of Toronto, City Clerk's Office. (2018). [Duty to Documenting Fact Sheet](#)
- City of Toronto, City Clerk's Office. (2023). [Electronic Records Disposition Guideline](#)
- City of Toronto, City Clerk's Office. (2021). [File Planning 101 Guideline](#)
- City of Toronto, City Clerk's Office. (2023). [Information Management Accountability Policy](#)
- City of Toronto, City Clerk's Office. (2023). [Information Protection Classification Framework](#)
- City of Toronto, City Clerk's Office. (2023). [Information Protection Classification Standard](#)
- City of Toronto, City Clerk's Office. (2018). [Municipal Code Chapter 217, Records, Corporate \(City\)](#)
- Province of Ontario. (R.S.O. 1990). [Municipal Freedom of Information and Protection of Privacy Act](#)
- City of Toronto, City Clerk's Office. (2022). [Protection of Privacy Policy](#)
- City of Toronto, City Clerk's Office. (2008). [Records Management Metadata Standard](#)
- City of Toronto, City Clerk's Office. (2023). [Schedule A – Records Retention Schedule, Chapter 217 of the Toronto](#)
- City of Toronto, City Manager's Office. (2019). [Corporate Strategic Plan](#)
- City of Toronto, Office of the Chief Information Security Officer. (2023). [Access Management Policy](#)
- City of Toronto, Office of the Chief Information Security Officer. (2021). [Mobile Device Management Policy](#)
- City of Toronto, Technology Services Division. (2018). [Acceptable Use Policy](#)
- City of Toronto, Technology Services Division. (2023) [Enterprise IT Disaster Recovery Policy](#)

8. Contact

For assistance regarding collaboration tools, contact Corporate Information Management Services at cisp-consults@toronto.ca.

9. Guideline Approval

Approval provided by Kristie Pratt, Deputy City Clerk, effective December 8, 2023.

10. Guideline Review

The City Clerk's Office will review this Guideline and its effectiveness as warranted.

Appendix

Appendix A: Definitions

Application: An application, also referred to as an application program or application software, is a computer software package that performs a specific function directly for an authorized user or, in some cases, for another application. An application can be self-contained or a group of programs.

Application Administrator: role with elevated permissions responsible for the overall enterprise maintenance of an application including processes and methodologies for maintaining, enhancing, and managing the application.

Authorized Users: are all individuals who have been granted access to the City's Information Technology Assets. This includes, but is not limited to, employees, consultants, contractors, subcontractors, individuals on secondment to the City, students and volunteers at the City of Toronto and Accountability Officers and anyone working or volunteering for or in their Offices subject to Section 3-10 F(5), Chapter 3, Accountability Officers, of the Toronto Municipal Code.

Classification: An activity comprised of grouping similar or related things (concepts or terms) together; separating dissimilar or unrelated things; and arranging the resulting groups into a logical sequence.

Collaboration Tool: Applications or software features that support collaborative business activities such as writing documents, having discussions, tracking project performance, brainstorming (ex. whiteboarding) or tracking issue tickets.

City Record: Recorded information created or received in the course of City administration or delivery of City services.

Deletion: the obliteration or destruction of specific information.

Disposition: the actions taken with regard to inactive City records as determined by an appraisal pursuant to legislation, regulation, or administrative procedure. Actions include destruction, designation as archival records, or as designation as permanent records.

Duty to Document: A statutory responsibility for all City employees and officials to create full, accurate, and complete records of service delivery activities and business decisions, regardless of how they were originally communicated.

Metadata: data describing context, content and structure of records and their management of through time.

Migration: the process of moving records, including their existing characteristics, from one hardware or software configuration to another without changing the format.

Recordkeeping Repository: a shared filing system in which records, including data and images, are captured, protected, retained and destroyed in accordance with approved records retention schedules. A recordkeeping system, when used in conjunction with recorded policies and procedures, defined roles and responsibilities, and ongoing training, constitutes an appropriate system for managing government information.

Retention Schedule: An authority comprising of a description of a body of records, a retention period for those records and a disposition rule stating whether, at the expiry of the retention period, the records are to be destroyed or preserved by Archival Services.

System: A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Transitory Information: Information in any format that are of short-term value, required solely for the completion of a routine action or the preparation of a record. It is not required to meet statutory obligations or to sustain administrative or operational functions.

Workspace Administrator: role responsible for the management, utilization and protection of the application workspace and its data.