

Information Management Guideline – Email Management

Guideline No.: CIMS-G026

Version No.: 1.0

Issued On: January 13, 2026

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

Subject: Information Management

Keywords: Email, Outlook, information technology, 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 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:**
 - City Clerk's Office
 - Corporate Information Management Services (Corporate Information Strategy & Policy, Records Services, Privacy & Information Collection, and Archival Services)
 - Members Services and Program Support (Business & Technology Planning)
 - Technology Services
 - 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) 803-9140

Kristie.Pratt@toronto.ca

Contents

Information Management Guideline – Email Management	1
1. Introduction	3
2. Purpose	3
3. Application	4
4. Scope	4
5. Principles	4
6. Guideline: Email Management	7
7. References	10
8. Guideline Approval	11
9. Guideline Review	11
Appendix	11
Appendix A: Definitions	11

1. Introduction

Email is an electronic communication tool that is assigned to most City of Toronto employees, and in certain circumstances, to volunteers and contracted vendors of the City. Email accounts are assigned to individuals during their employment with the City, either as an individual mailbox or as generic shared mailboxes that can be accessed by multiple users to support a business activity.

Responsible information management practices and privacy protections must be implemented into the use and management of City email accounts. City staff have a responsibility to manage and safeguard email as they do with other City records. Accountable email management includes the identification of emails that are business records and ensuring that they are managed in accordance with responsible recordkeeping principles. It is important for all City staff to be aware of their responsibility to properly safeguard the City's records, including protecting any [personal and confidential information](#) contained in email messages.

Good email management helps City staff deliver on the [Corporate Strategic Plan](#)'s vision for A Well-Run City by fostering trust and confidence in local government and ensuring:

- Business decisions made over email are stored and documented in designated City records repository systems (e.g. shared network drives, SharePoint, etc.), so that government administration and service delivery remains accountable.
- Emails are accessible (as appropriate) to support an open and transparent government (e.g. freedom of information requests, etc.).
- Users employ appropriate privacy and security practices to protect City information and any personal or confidential information contained in email.

2. Purpose

The purpose of this guideline is to provide an overview of information management responsibilities for authorized City users with access to the City's email system, assist staff in differentiating between transitory records and City business records in email form, and outline information management best practices when utilizing email in the performance of professional duties.

This guideline supports implementation of the [Information Management Accountability Policy](#), [Responsible Record Keeping Directive](#), [Protection of Privacy Policy](#), [Cyber Security Policy](#), and [Acceptable Use of Information and Technology Assets Policy \(AUP\)](#).

3. Application

This guideline applies to all City Divisions and authorized users of the City's email system, including City employees, volunteers, and third parties who access, create, store and use email in the course of their duties.

This guideline does not apply to Elected Officials, Accountability Officers, or City Agencies and Corporations. However, Elected Officials are responsible for keeping those emails (and other forms of records) relating to their constituency files and to City business separate. The City of Toronto encourages Agencies and Corporations to review and use this guideline as it suits their business needs.

This guideline applies to the City's email system and emails accessed on or used within City technology assets in accordance with the [Acceptable Use of Information and Technology Assets Policy \(AUP\)](#).

4. Scope

This guideline addresses the management of email messages and their attachments as business records. Specifically, this guideline addresses email messages generated and received by City staff and/or volunteers in the performance of their professional duties. For guidance on other forms of digital communications (e.g. instant messaging), please see the Guideline on [Managing Information in Collaboration Tools](#).

The guideline strives to set standards for information protection and recordkeeping regarding the use, storage, and transmission of email. Email accounts assigned to applicable individuals include individual City email accounts and generic shared mailboxes.

5. Principles

When using email, City staff are expected to:

- **Identify** – Determine if an email is a business record or a transitory record. If a business record, it will be subject to retention and disposition requirements outlined in Chapter 217 of the City of Toronto's Municipal Code.

- **Retain** – Store business record emails in their division's designated records repository.
- **Protect** – Safeguard emails that contain personal or confidential information.
- **Dispose** – Dispose emails in the appropriate manner prescribed in the retention schedule.

The City's Email System is a Corporate Asset

Email use is essential in facilitating communication for service delivery and business operations at the City of Toronto. Email allows City staff to efficiently exchange information, provide approval or endorsement of work direction, coordinate activities, and maintain relationships with clients, vendors, and partners. The City's email system involves integrated applications, primarily Microsoft Exchange Online and Microsoft Outlook (front-facing client application), to conduct the following functions:

- Sending and receiving email messages
- Managing calendars
- Scheduling meetings
- Managing email distribution lists

The City's email system is an Information Technology Asset comprised of mailboxes which are assigned to authorized users of the City of Toronto.

As a corporate resource and tool, access and availability to assigned email is not permanent and can be suspended or terminated. Email is to be used in accordance with the City's [Acceptable Use of Information and Technology Assets Policy \(AUP\)](#) and any applicable federal or provincial legislation. This does not negate the professional and ethical use of email as per [City's Toronto Public Service By-Law, Toronto Municipal Code, Ch. 192](#).

Emails Are Records

Emails, and email attachments are considered records under the [City of Toronto Act](#) and [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#). If identified as a business record, the email and its associated contents are subject to retention requirements under the [City of Toronto Municipal Code Chapter 217](#) and to access and privacy requirements under MFIPPA.

Email systems such as Microsoft Exchange Online (Outlook) were not designed to house and manage business records in a manner that aligns with the City's recordkeeping obligations. Migrating emails that are business records from a personal email account to a shared network drive or other divisional records repository supports the City's recordkeeping obligations and [duty to document](#), ensuring that information is retained and made accessible to staff and the public as appropriate.

City staff are responsible for moving emails that constitute City business records from Outlook to the divisionally designated recordkeeping repository, such as:

- Shared network drive (e.g. G:/ Drive)
- SharePoint site
- Electronic document and records management system (e.g. T-Recs)
- Business application (e.g. Salesforce, etc.)

Please consult with divisional management as to the appropriate repository for email storage in your business unit.

Emails are Subject to Retention and Disposition

Emails should be retained and disposed of according to the City's records retention and disposition schedule. Authorized email users are responsible for distinguishing between business records (which need to be retained) and [transitory records](#) (which can be disposed of after serving their purpose).

The deletion of transitory records (emails) from a user's inbox that are no longer needed is a valuable step in email management. Emails and associated attachments that constitute authoritative business records must be saved by the user in the appropriate divisional recordkeeping repository to adhere to the City's records retention schedule.

User email accounts and associated contents within are governed by the retention policies established in the City's [Records Retention Schedule, code I0345](#). Technology Services Division has established automatic deletion of email messages once the appropriate retention period has passed. All messages in the email system that are received, sent, user-deleted (transitory or not), and archived will be retained for 7 years for employees and contract staff at the level of Manager or below, or 10 years for Executives and Senior Management after they have left their appointed role. Individual emails and associated contents identified as official business records must be migrated into divisional recordkeeping repositories and retained in accordance with the retention classification that aligns with that email's content.

The City offers an email archive function for older emails to support legal holds, investigations, and disaster recovery planning. Email archiving does not satisfy recordkeeping obligations because the City's email archive can only be accessed by a small number of IT administrators and authorized users. City staff are still required to store email messages with business value in their division's shared drive (or other records repository) to support business continuity.

If you are unsure how to identify a transitory record from a business record, speak to your management or contact Corporate Information Management Services [Record](#)

[Services Contact](#) for guidance and see further detail below on [identifying transitory records](#).

Access

Individual City email accounts or [generic shared email inboxes](#) are neither private nor permanent and are subject to corporate access depending on the circumstance. Generic (shared) email mailboxes by default are accessible to the assigned authorized users and the primary account holder.

All email messages sent, received, deleted, or maintained by City staff are the property of the City of Toronto, and are subject to MFIPPA and the [Toronto Municipal Code](#). Emails may be requested for:

- Freedom of Information (FOI) requests – Under MFIPPA, email messages can be requested by the public. Emails within the custody and control of the City will be reviewed by the Access to Information team upon receipt of an FOI request, subject to the limited access exemptions and exclusions outlined in the Act. The City Clerk's Office processes FOI requests and works with the division to locate responsive records. Individuals are required to cooperate by searching and producing any requested emails within the legislated timelines.
- Investigations and Audits – Third-party access to email accounts may be granted to support investigative requests. Investigative requests are often sent directly to Technology Services Division (TSD), and requests can originate from a Division Head, Legal Services, the Office of the Chief Information Security Officer, or an Accountability Officer's Office.

6. Guideline: Email Management

The City's [Information Management Framework](#) commits staff to managing information as a corporate asset. Effectively managing email supports compliance with City policies and legislation such as MFIPPA and the Municipal Code Chapter 217, minimizing the risk of privacy breaches and helping prevent financial and reputational damage to the City. Maintaining City business records in your division's recordkeeping repository ensures consistent accessibility, supports the application of proper retention schedules, and helps streamline the Freedom of Information process when requests are received. Adopting best practices, where possible, should be seen as part of the ongoing commitment to the secure and effective use of email.

Best Practices when Sending/Receiving Email

- Consider the following when evaluating email use:

- Purpose (goal) of email communication
 - Whether or not the email constitutes as a business record
 - Whether the information shared via email constitutes as personal, confidential or sensitive information
 - The need to use a secure alternative when sharing personal or confidential information as regular email is not encrypted
-
- All staff with @toronto.ca email addresses are required to follow and use the City's [email signature standards](#) for internal and external communications. Consistent email signatures help ensure that every message from the City looks professional and includes the correct contact information.
 - Subject lines of emails should never include personal information, personal health information, or confidential information.
 - Before sending, review all email attachments for accuracy and any potential for unintended disclosure of confidential, personal information, or personal health information.
 - Always review the recipient fields to ensure email addresses are entered correctly and in the appropriate fields, "To", "CC", or "BCC". While emails to fellow staff can be recalled, City staff are unable to retract an email if it has already been opened by recipient.
 - Personal email addresses are considered personal information and as such only send emails (via "To", "CC", "BCC") to individuals that require the email communication.
 - Assess if you require Auto-Complete turned on to suggest names when typing in the "To", "CC", or "BCC" fields. Consider emptying the Auto-Complete list regularly in Outlook to prevent the inclusion of unintended email recipients.

Email Usage – Recordkeeping, Access & Privacy Best Practises

- Assess whether the email is a City business record by asking if it relates to:
 - Business processes and transactions
 - Communications and consultations with stakeholders and partners
 - Management approvals provided via email
 - Justification of actions or decisions
 - Audit, legal, or FOI requests
 - Complaints related to City services
 - Contains any attachments – or links to – City records.

- Maintain the authenticity and integrity of an email record by preserving all content associated with an email message, including its body text, attachments, calendar invites, and metadata (such as sender and recipient email addresses) when storing in your business unit's records repository.
- Consult with CIMS' Record Services unit to ensure email-generated business records are properly filed and stored in records file plans (subject to disclosure and retention requirements). This includes storing sensitive or confidential email content in access-controlled repositories to protect privacy and prevent unauthorized access.
- Transitory email records should be deleted from the inbox when they're no longer relevant. They do not need to be stored in a City records repository. Examples of emails that are transitory include:
 - Personal and non-work-related emails, such as lunch confirmations or congratulatory messages
 - Duplicate messages and duplicated email threads
 - Corporate communications received from City accounts such as Strategic Communications
 - System generated communications, such as IT password reset requests
 - Unsolicited marketing materials
- Once a City business record email has been moved to an appropriate records repository, you can delete the copy stored in the inbox.
- Consult with CIMS, your divisional management, Health Information Custodian (HIC), or Privacy Unit (privacy@toronto.ca) for a consultation when transmitting personal or personal health information via email.
 - Your divisional Client Relationship Manager (CRM) from Technology Services Division (TSD) can also help you determine whether a City approved secure file transfer tool be more appropriate than email to share or transfer personal or confidential information.
- Use City email accounts appropriately and securely:
 - Do not use personal email accounts for City business
 - Do not use City email account for personal purposes that are unrelated to your work or business with the City.
 - Do not grant other users unauthorized access to your designated City email account
- Comply with appropriate privacy and security obligations when handling sensitive information, personal information or personal health information:

- If you're collecting personal information via email, please refer to the [What You Need to Know About Collecting Personal Information Fact Sheet](#) and the [Understanding Notice of Collection Statements Guideline](#).
- Follow the [Privacy Breach Protocol](#) should there be a breach or suspected breach of personal information or personal health information when using City email accounts.
- Use the "Report Phishing" feature in Outlook to report suspicious email. Do not respond, forward to colleagues, or click on email phishing scams. Learn how to spot the signs of phishing and other cyber security concerns on the [Cyber Intel](#) page.

Information Management Best Practices for Generic Shared Mailboxes

- Generic shared mailboxes should have primary management oversight and a designated mailbox owner. Divisional teams are encouraged to establish their own onboarding and offboarding policies and procedures to inform staff of their obligation to identify, retain, protect, and dispose of emails in the shared inbox.
- Primary account owners of generic shared mailboxes should monitor access permissions and request that access permissions be removed promptly once a user is no longer in the role or has a responsibility for use of the shared mailbox.
- Users of a generic shared mailbox should never share and/or delegate access unless specifically authorized by the primary mailbox owner and/or management lead.

7. References

- [Municipal Code Chapter 217, Records, Corporate \(City\)](#)
- [Acceptable Use Policy](#)
- [Information Management Accountability Policy](#)
- [Responsible Record-Keeping Directive](#)
- [Transitory Records Fact Sheet](#)
- [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#)
- [Personal Health Information Protection Act \(PHIPA\)](#)
- [Schedule A – Records Retention Schedule, Chapter 217 of the Toronto Municipal Code.](#)
- [Canadian Copyright Act](#)
- [City Clerk's Office: Information Management Framework \(IMF\)](#)
- [Protection of Privacy Policy](#)

- [Cyber Security Policy](#)
- [City's Toronto Public Service By-Law, Toronto Municipal Code, Ch. 192](#)

8. Guideline Approval

Approval provided by Kristie Pratt, Deputy City Clerk, effective January 13, 2025.

9. Guideline Review

The City Clerk's Office will review this Policy and its effectiveness at the two-year mark from the effective date of this Guideline, or earlier if warranted.

Appendix

Appendix A: Definitions

Authorized Users: 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.

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.

Confidential Information: Information in the possession of or received in confidence by the City that the City is either prohibited from disclosing, or is required to refuse to disclose, under the Municipal Freedom of Information and Protection of Privacy Act, or other legislation. Includes, but is not limited to, privileged information, draft by-laws or staff reports, third party information, personal information, technical, financial or scientific information and any other information collected, obtained or derived for or from City records that must or may be kept confidential under the Municipal Freedom of Information and Protection of Privacy Act, the Personal Health Information Protection Act, or the City of Toronto Act.

Deletion: The erasure of specific information.

Disposition: The actions taken with regards 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.

Freedom of Information Request: Formal requests for records of the City of Toronto. FOI requests should not be submitted for information that is already available on the City website, from a City division by request, or for information that is held by other governments or government agencies. Information Management – The means, by which the City of Toronto responsibly plans, creates, captures, organizes, protects, uses, controls, shares, disposes, and evaluates its information (including records, data, and digital images), and through which it ensures that the value of that information is identified and used to the fullest extent.

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

Personal Information: Recorded information about an identifiable individual, such as (but not limited to): address, race, religion, gender, family status, employment history, medical history, blood type, DNA, any identifying number assigned to the individual, personal opinions or views of an individual about another individual, correspondence of a personal or confidential nature from an individual. For more information, refer to the personal information interpretation under MFIPPA, S.2

Record: Information, however recorded or stored, whether in printed form, on film, by electronic means or otherwise, and includes documents, financial statements, minutes, accounts, correspondence, memoranda, plans, maps, drawings, photographs, and films – City of Toronto Act, 2006, s.3 (1).

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.

Transitory Record: Information in any format that is 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.