Information Management Guideline – Personal Drive Management

Guideline No.: CIMS-G025

Version No.: 2.0

Issued On: October 20, 2025

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

Subject: Information Management

Keywords: personal drives, OneDrive, records management, information technology

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) 392-9683
Kristie.Pratt@toronto.ca

Contents

1. Introduction

The City of Toronto provides Personal Drive space for all staff to use during their time of active employment. This Personal Drive space allows for the storage of records that are transitory and/or personal business records, or a combination of both. It allows staff to store and access files from any City device that is connected to the internet. Personal Drives are primarily intended for management of a user's personal business records. City of Toronto staff have used H:/ Drives or more recently OneDrive as their Personal Drive space.

Personal business records are records related to the employee that are created during the course of their employment with the City and does not pertain to city business. Personal business records may include and not limited to the following of the individual employee user of the Personal Drive:

- resumes and cover letters
- eTime approvals
- personal performance planners
- receipts
- tuition reimbursement requests
- certifications
- eLearning completion documentation
- applications for leaves of absence
- job-specific onboarding materials and reference materials related to job function
- other

The storage space on Personal Drives is limited as they are not meant to store authoritative City records. City records must be correctly identified (classified), organized, and managed throughout their lifecycle as part of good records and information management practices. It is the responsibility of staff to regularly review the records in their Personal Drive and migrate any authoritative City records to the appropriate divisional recordkeeping repository(s) and delete transitory or personal records that are no longer needed.

The City has specific security requirements for all City information stored on the City's technology assets as per the City's Cyber Security Policy. The preservation of business records must adhere to the legislated obligation for the City to maintain records under its custody or control as established under Chapter 217, the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), and the Personal Health Information and Protection Act (PHIPA). The City maintains the public's right to access information that can be easily searched and retrieved by ensuring records under the stewardship of the City are accessible.

2. Purpose

This guideline provides City of Toronto staff with principles and best practices for Personal Drive management, including an overview of information management responsibilities for Personal Drives. This guideline covers the importance of Personal Drive management as it pertains to personal business records and does not cover other responsibilities of staff for accountable management of City records in accordance with Toronto Municipal Code, Chapter 217, Records Corporate.

This guideline also builds on the City's Information Management Accountability Policy and its commitment to managing information throughout its lifecycle, from creation or collection to disposition. Other relevant policies, bylaws, and legislation that set out employee responsibilities for managing City Records include:

- City of Toronto Act
- Toronto Municipal Code, Chapter 217, Records, Corporate (City)
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Personal Health Information Protection Act (PHIPA)
- Information Management Accountability Policy
- Responsible Record Keeping Directive
- Acceptable Use Policy

3. Application

This guideline applies to all City of Toronto Divisions, City staff, volunteers, and contract staff hired by the City of Toronto who have been assigned a Personal Drive. The guidance is for managing information in Personal Drives only and does not apply to the management of local drives such as desktop folders or shared drives such as network drives and SharePoint.

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 guideline appropriate to their business circumstances.

4. Best Practices

The following best practices ensure that regular oversight is applied to personal drives and that their usage is limited to personal business records and/or transitory records. All staff are expected to carry out their responsibilities managing City information according to the principles outlined in the Information Management Accountability Policy. The public expects an accountable and transparent government where records can be readily accessible upon request and key business decisions are appropriately documented, outside of drives only accessible to one individual.

Accountability & Acceptable Use of Personal Drives

- Adhere to Toronto Public Service By-Law responsibilities and obligations to remain professional, ethical, and impartial as an employee of the public service and commitment to its values.
- Do not save anything contrary to the Acceptable Use Policy. Personal Drive space is intended for personal business records created in a professional capacity.
- Personal Drive use is subject to the Acceptable Use Policy, which states:
  - Authorized [City] Users shall not expect absolute privacy when using the City's Information Technology Assets, including such limited personal use as permitted in accordance with Section 7 of this Policy.
  - All information and records created or legally acquired using the City's Information Technology Assets are the sole property of the City of Toronto with the exception of records which arise from the permitted personal use of Information Technology Assets.
  - Authorized [City] Users are responsible for properly managing personal files. The City is not liable nor will it incur any expense to protect or back up personal files.
  - Authorized [City] Users are encouraged to not store their own personal information or personal files on the City's Information Technology Assets. Users that elect to store their own personal information or personal files acknowledge that they are doing so at their own risk.

Privacy when Using Personal Drives

- Avoid storing personal information or files on City IT assets.
- For people managers, confidential employee information must be stored in access-controlled shared locations or another approved repository, not one's personal drive. For assistance in setting up a secure location for these types of records, contact your divisional or corporate IT team to set up an access-controlled location and contact the division's Records Services Contact for guidance on file organization for people management records.

Records Management and Personal Drives

- Save City business records in the appropriate repository in adherence to proper retention and disposition requirements, not in a personal drive space.
- Personal Drives are for personal business records only (e.g., resumes, eTime approvals, certifications).
- Transitory records should be deleted promptly; authoritative records that begin as drafts in your personal drive must be migrated to appropriate repositories upon completion of a final version.
- Ensure that you can identify a City business record relative to a transitory record. When needed, consult divisional management or Records Services for help identifying and managing records.
- Transitory records should be deleted promptly; authoritative records that begin as drafts in your personal drive must be migrated to appropriate repositories.
    - Personal Drives are set at a limited storage capacity. Once this limit is reached, staff will be unable to add additional files. Staff must manage records in their Personal Drive for storage, transfer/migration, and deletion.
    - Employees should never store authoritative City business records or personal business records on their desktop or local drives because these areas are not backed up and cannot be recovered if there is hardware failure.

Access & Oversight of Personal Drives

- Personal Drives are assigned to a primary user. Although by default they are only visible and accessible to that authorized City user and select IT administrators, that user may choose to grant access to certain files or folders (in their OneDrive) to other City staff.
- There may be instances where third-party access to other City staff may be is granted to a Personal Drive. To initiate an internal third-party access request, contact Corporate Services' File Services team (Technology Services Division). Third-party access to Personal Drives is only granted to support:
    - Business requests: Including requests to review the Personal Drives of former employees where business records may be retained. Business requests for access require approval from both the business director and file services director.
    - Investigative requests: Including requests to review the Personal Drive of an employee (current or former) who is subject to legal investigation or inquiry. Investigative requests for access must originate from Legal Services, the Office of the Chief Information Security Officer in accordance with the Acceptable Use Policy – User Monitoring Procedures, or an Accountability Officer's Office.
    - Freedom of Information (FOI) requests: Personal Drives can also be subject to access via FOI requests as MFIPPA establishes a general right to the information held by governments and institutions. If authoritative City records

are saved in a Personal Drive and these records are requested for a FOI, then owners (or a designate) of the Personal Drive are expected to retrieve these responsive records.

- Assigned users are responsible for the ongoing use, maintenance, and any migration of their Personal Drive content.

Non-Permanency & Offboarding

- Personal Drives are assigned by the City for limited temporary use and are not intended for permanent storage.
- When an individual leaves the City or becomes inactive (e.g., is on leave), their license to their Personal Drive will be revoked and deactivated after a period (generally within 30 days) in which its contents will be read-only. After a period of read-only access, its contents will be permanently deleted.
- Divisions should provide onboarding and offboarding checklists to support employee oversight and accountability for the information management of Personal Drives. Management may reference Information Management Responsibilities for Employee Crossboarding and Offboarding Guideline and Manager and Supervisor Information Management Responsibilities for Employee Onboarding, Crossboarding and Offboarding Guideline
- For staff that are moving between Divisions and losing their Personal Drive (OneDrive or H:\ drive) in the process (due to receiving a new user id), it is their responsibility to migrate all personal business records to their new Personal Drive.
- When employees move divisions, retire, go on leave, or leave the City, they are responsible for completing the Exiting Employee Information Management Checklist, which supports knowledge transfer, technology asset management, and information disposition. If a former employee does not complete the Exiting Employee Checklist, it is the responsibility of their reporting manager to make a business request for Personal Drive access in a timely manner, review the contents, and migrate any City business records to a shared repository prior to the purging of the Personal Drive.
- For those employees losing access to their Personal Drive due to an impending leave of absence, they may email personal business records to their City email to ensure future access upon their return to the office or transfer them to a City-approved USB drive. Staff should consult their management, local IT, or Technology Services for guidance.

5. References

- Municipal Code Chapter 217, Records, Corporate (City)
- Toronto Municipal Code, Chapter 192
- Acceptable Use Policy
- Information Management Accountability Policy
- Responsible Record-Keeping Directive
- 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.
- City Clerk's Office: Information Management Framework (IMF)
- Protection of Privacy Policy
- Information Management Responsibilities for Employee Crossboarding and Offboarding Guideline
- Cyber Security Policy

6. Guideline Approval

Approval provided by Kristie Pratt, Deputy City Clerk, effective October 20, 2025.

7. 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 A: Definitions

City Record: A record created or received during City administration or delivery of City services. Also includes records that were created or received by the City of Toronto's predecessor municipalities' administration or service delivery. This includes records created, accumulated, and used by a member of Council executing their responsibilities imposed on members of Council under the City of Toronto Act, 2006.

Disposition: The final step in the active lifecycle of records, including records destruction and transferring for permanent preservation.

Freedom of Information Request: Formal requests for records from the City of Toronto. FOI requests should not be submitted for information that is already available on the City's website, from a City division by request, or for information that is held by other governments or government agencies.

Information Management: The means used by the City of Toronto to responsibly plan, create, capture, organizes, protect, use, control, share, disposes of, and evaluates its information resources, and how it ensures that the value of that information is identified, trusted, and used to the fullest extent.

Record: An information resource, however recorded or stored, whether in printed form, on film, electronic or otherwise, including documents, financial statements, minutes, accounts, correspondence, memoranda, plans, maps, drawings, photographs, and films.

Personal Business Record: A record created by a staff member relating to themselves in a professional capacity.

Personal Information: Recorded information about an identifiable individual, including:

1. information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual
2. information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved
3. any identifying number, symbol or other particular assigned to the individual
4. the address, telephone number, fingerprints, or blood type of the individual
5. the personal opinions or views of the individual except if they relate to another individual
6. correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence

7. the views or opinions of another individual about the individual
8. the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual

Recordkeeping repository: A physical or digital storage area where documents and records are kept. Repositories can be integrated with other applications so various electronic documents and records can be searched and accessed in one location.

Retention Schedules: 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: City records that are only needed for a short period of time. They may be copies of records, or records that others have created. Transitory records have no value after an immediate or minor transaction and can be discarded when they are no longer useful.

Retention Period: The length of time records should be maintained in a certain location or format for administrative, legal, fiscal, historical, or other purposes.