

Information Management Guideline – Information Management and Privacy in an Open Office

Guideline No.: CIMS-G016

Version No.: 1.1

Issued On: November 14, 2023

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

Subject: Information Management and Privacy in an Open Office - Guideline

Keywords: records management, information management, open office, privacy

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:** Privacy and Information Collection, Strategy & Policy, Records Services.

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 – Information Management and Privacy in an Open Office 1

1	Introduction	3
2	Application.....	3
3	Purpose.....	4
4	Guidelines for Information Management and Privacy in an Open Office.....	4
4.1.	Record keeping.....	4
4.2.	Information Privacy	4
4.3.	Secure Disposition	5
4.4.	Touchdown Floors.....	6
5	References	6
6	Contact.....	7
7	Guideline Approval	7
8	Guideline Review	7
	Appendices.....	8
	Appendix A: Definitions	8
	Appendix B: Clean Desk Checklist.....	10

1 Introduction

The City of Toronto is modernizing its work locations toward a shared open office environment. This new work environment supports greater communication and creativity between employees and introduces new challenges in ensuring that proper privacy and recordkeeping obligations are met.

Information management and privacy responsibilities remain consistent whether an employee works outside the workplace, in a traditional City work location, or in an open office environment. The [Information Management Accountability Policy](#) highlights the duty of employees to manage and safeguard all City records, including those with personal and confidential information as defined by the Municipal Freedom of Information and Protection of Privacy Act ([MFIPPA](#)).

Applying good record-keeping and privacy practices helps ensure that records are managed efficiently throughout their lifecycle in compliance with City legislation, policies, and standards, while maintaining continued access to records for those who need it.

This guideline advises staff on how to properly manage information and safeguard privacy in an open office environment and provides a checklist to ensure a clean desk at the end of the workday. An open office environment may involve staff sharing workstations, increasing the risk around improper handling of City records.

When an employee is working remotely outside of a City workspace, the [Remote Work – Information Management and Privacy Guideline](#) provides instructions and helpful tips to ensure employees are creating, storing, using, and managing City records appropriately.

2 Application

This guideline applies to all City of Toronto employees that are working in an open office environment.

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.

3 Purpose

The purpose of this document is to guide City of Toronto employees to apply record keeping, privacy, and secure information disposal practices in an open office environment to ensure legislative compliance.

4 Guidelines for Information Management and Privacy in an Open Office

4.1. Record keeping

It is vital that records are managed with access and records lifecycle requirements in mind when working in an open office with shared workstations. This includes preventing the unauthorized access, sharing, and/or destruction of City records, and safeguarding personal and sensitive information contained within those records.

For these reasons, it is important to:

- Store physical records securely in the filing cabinets assigned to your unit.
- Dispose of [transitory records](#) promptly once they are no longer useful to you and your team. Do not keep or store transitory records past their usefulness.
- Review physical records annually and [transfer inactive business records](#) (records that have reached the end of their active retention) to the Records Centre. Contact [Records Services](#) for more information on managing your records.
- Dispose of post-it and other daily notes safely at the end of your workday and ensure that nothing is left in the printer area.
- Keep physical records on City property.
- Be familiar with your responsibilities for the proper management of City records.

4.2. Information Privacy

Working in an open office and sharing workstations introduces new challenges in terms of protecting personal and confidential information. Staff must be aware of these challenges, taking appropriate measures to reduce the level of risk.

Staff should follow these best practices:

- Be aware of your confidentiality obligations before accessing or using any information while working in a shared workspace. Ensure that records storage and safeguards match the nature and level of sensitivity of the information contained in the records. The [Information Protection Classification Standard](#) can provide support on this matter.
- Do not leave sensitive information where it can be vulnerable. When leaving your

workstation for any reason and amount of time, secure documents in your unit's assigned file cabinets.

- Lock your computer when stepping away from your desk.
- Do not share your password with anyone; use your computer's screen-saver option and password protection features.
- Lock filing cabinets with records containing personal information when not in use or when leaving your work area.
- Employ privacy protecting technologies provided by the City, including headphone telephony, screen protectors and, screen saver technology.
- Be aware of accidental disclosure of personal information from monitors and shoulder surfing.
- Take sensitive calls in a phone room or other enclosed space and be aware of your surroundings when dictating or collecting personal information on the phone, in person, and on video calls.
- Book meeting rooms for sensitive discussions or confidential meetings with your colleagues.
- Transport City devices and records between floor or city buildings in a secure manner and do not leave them unattended.

4.3. Secure Disposition

The City of Toronto maintains a commitment to data stewardship and secure handling of all City records through their lifecycle. This custody of information requires secure handling of a record from its creation until it is destroyed. As such, all staff are expected to ensure that records and information are disposed of in the appropriate manner, according to the [City's Records Retention Schedule](#).

In an open office environment:

- Shred all transitory paper records containing personal or personal health information using a crosscut style shredder or disposing of them in a locked confidential bin.
- Use open recycle bins only for non-sensitive transitory records.
- Submit a service request to [FRED](#) if your work location does not have a secure disposal bin on your floor or if the bins are full and need to be emptied.
- Electronic devices storing information must be disposed of in compliance with the [Confidential Waste Disposal Policy](#) and [Information Technology Asset Management Policy](#) and the Technology Services Division (TSD)'s directives on secure disposal. Please contact TSD for more information.

4.4. Touchdown Floors

Touchdown floors are floors that are not assigned to a specific division. They are open to City employees of various business areas or divisions who would like to use an available meeting or collaboration space or need to work for all or part of the day from a different location than their base office.

These floors are not equipped to store physical records or receive mail. It is expected that all desks and lockers are left clean and empty at the end of the day.

If you are working on a touchdown floor, it is recommended that you:

- Do not bring physical records to these floors unless authorized to do so. If authorized, ensure those records are safeguarded and then returned to their assigned divisional storage area when the work is complete.
- Use privacy protective technology provided by the City, including headphones, headset, screen protectors and, screen saver technology.
- Lock your computer when stepping away from your desk.
- Be aware of accidental disclosure of personal information from monitors or shoulder surfing.
- Take sensitive calls in an available phone room or other enclosed space and be aware of your surroundings when dictating or collecting personal information on the phone, in person, and on video calls.
- Book meeting rooms for sensitive discussions or confidential meetings.
- Remove and/or properly dispose of all transitory paper records or printouts that you used before leaving at the end of the day.

5 References

- City of Toronto, People & Equity (2023). [Hybrid Work Policy](#)
- City of Toronto, City Clerk's Office (2023). [Information Management Standard – Information Protection Classification Standard](#)
- City of Toronto, City Clerk's Office. (2023). [Information Management Accountability Policy](#)
- City of Toronto, City Clerk's Office. (2023). [Information Protection Classification Standard.](#)
- City of Toronto, City Clerk's Office. (2022) [Protection of Privacy Policy](#)
- City of Toronto, City Clerk's Office (2021). [Working Remotely - Information Management & Privacy Guideline](#)

- City of Toronto, City Clerk's Office (2021). [Transitory vs Business Records Decision Tree](#)
- City of Toronto, City Clerk's Office (2021). [Transitory & Business Records Infographic](#)
- City of Toronto, City Clerk's Office. (2018). [Transitory Records Fact Sheet](#)
- City of Toronto, Corporate Real Estate Management. (2018). [Confidential Waste Disposal Policy](#)
- City of Toronto, City Clerk's Office. (2011). [Responsible Record-Keeping Guideline](#)
- City of Toronto, Technology Services Division. (2011). [Information Technology Asset Management Policy](#).
- Government of Ontario. (2004). [Personal Health Information Protection Act, 2004](#)
- Government of Ontario, City of Toronto. (1990). [Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990](#)
- [FRED Service Request System](#).

6 Contact

For assistance regarding information management and privacy in an open office, contact Corporate Information Management Services at cisp-consults@toronto.ca

7 Guideline Approval

Approval provided by Kristie Pratt, Deputy City Clerk, effective November 14, 2023

8 Guideline Review

The City Clerk's Office will review this Policy two years after the effective date of this Guideline, or earlier if warranted.

Appendices

Appendix A: Definitions

Business Record: recorded information created, received, and maintained as evidence, and as an asset by the City, in pursuit of legal obligations, or in the transaction of business.

City Work Location: an employee's regular assigned City work location, where the employee typically reports for work during regular business operations. Examples include:

- City Hall, Metro Hall and Civic Centres
- Shelters, Seniors Services & Long-Term Care Homes
- Yards
- Division-specific leased and/or free-standing buildings (e.g. treatment plant, Fire Station)

Confidential Information: this 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 \(MFIPPA\)](#), the [Personal Health Information Protection Act \(PHIPA\)](#), or the [City of Toronto Act](#).

Hybrid Work: a workplace model that enables eligible employees to perform their work duties alternating between their City work location and a remote work location. Hybrid work is not fully remote.

Information Management Lifecycle: a model of records management and archival science that characterizes the life span of a record as comprising sequential stages: creation or receipt; classification; maintenance and use; disposition through destruction or transfer to an archival institution or agency; description in archival finding aids; preservation; reference and use.

Personal Information: as per MFIPPA, it is recorded information about an identifiable individual, such as (but not limited to) address, race, religion, gender, family status, employment history, medical history, any identifying number assigned to the individual, personal opinions or views of an individual about another individual, and correspondence of a private or confidential nature from an individual. Information about a person in an official, business or employment capacity is not considered personal information.

Remote Work: the performance of all or some of an employee's job duties at a remote work location, using technology to facilitate the performance of the employee's duties and access and communication between the employee and their people leader.

Remote Work Location: a non-City work location that allows the employee to perform their work safely, has network connectivity, and maintains security of City information appropriate to the work being performed. An employee's remote work location must be within a reasonable distance of their regularly assigned City work location, as determined by operational requirements, and within Ontario. Locations that offer public Wi-Fi or that are not private (coffee shops, malls, airports, libraries, etc.) are not considered suitable remote work locations.

Retention Period: the length of time that an organization is required to keep records.

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 the City Archives.

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

Appendix B: Clean Desk Checklist

This Clean Desk Checklist identifies the activities employees should conduct at end of the workday when working in an open office environment and/or at a shared desk to ensure information management and privacy obligations are met.

- ☐ Return physical records to your assigned filing cabinet or storage location.
- ☐ Lock your filing cabinets if you are the last person from your team to leave the floor.
- ☐ Remove all post-it notes from monitors and desk surfaces and securely dispose of them.
- ☐ Lock up any box of records that you were working on for the day in the assigned storage location.
- ☐ Check printers and scanners to ensure that no records or information are left behind.