Working Remotely - Information Management & Privacy Guideline

Guideline No.: CIMS-G011
Version No.: 2.0
Approval Date: May 2021

City Clerk's Office

An Information Management Guideline

Subject:	Managing Information Remotely	**Guideline No:** CIMS-G011 **Version No:** 2.0 **Effective:** 2021
Keywords:	Information, Management, Personal, Privacy, Records, Remote, Security, Work, WiFi, Telework, Access	
Issued By:	City Clerk's Office	
Revised on:	N/A	
Supersedes:	2020 1.0	
Approved By:	Kristie Pratt, Deputy City Clerk, Corporate Information Management Services, City Clerk's Office	
For more Information Contact:	Manager, Information Policy & Standards, Corporate Information Management Services, City Clerk's Office	

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.

Table of Contents

1. Introduction

Remote working has become a reality for many City of Toronto employees. Learning how to operate in a remote work environment has been both a challenge and an opportunity to rethink how the City delivers services, not just from the traditional office, but from any location.

While remote work allows City employees to have greater flexibility, there are specific responsibilities to protect privacy and manage City information that also apply to a remote workforce. Information management and privacy responsibilities do not change when an employee works outside the workplace. It is the duty of the employee to manage and safeguard all City records, including those with personal and confidential information. This guideline includes basic instructions and helpful tips to ensure employees are creating, storing, using, and managing City records appropriately when working remotely.

The outcomes of the guideline are to ensure that all City employees working remotely are:

- creating full and accurate records, and documenting business decisions
- filing or capturing records in a recordkeeping system as soon as possible
- preventing unauthorized disclosure, loss, or destruction of City records
- protecting personal, sensitive, and confidential information
- ensuring the disposal of records is authorized and properly documented

2. Application

This guideline applies to all City of Toronto Divisions, City staff, volunteers, and contract staff hired by the City of Toronto.

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. Information Management Responsibilities

City staff must manage records according to City policies, bylaws, and legislation, whether the records are created in the office, at the employee's home, or in another location. The Information Management Accountability Policy, and other relevant policies, bylaws, and legislation, set out employee responsibilities for managing City Records:

- Toronto Municipal Code, Chapter 217, Records, Corporate (City)

- City of Toronto Act
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)
- Personal Health Information Protection Act (PHIPPA)
- Emergency Remote Work Policy
- Information Management Accountability Policy
- Protection of Privacy Policy
- Secure Remote Access Use Agreement
- Acceptable Use Policy
- Corporate Cyber Security Policy

All City employees are expected to manage information according to the principles outlined in the Information Management Accountability Policy:

- Information is a valuable corporate resource that must be managed to improve openness and transparency in the delivery of City programs and services;
- Duty to Document requires all employees to create full, accurate, and complete records of all business activities, regardless of the communication methods and tools used;
- All employees share responsibility for the proper management of records and information and must provide timely access to records and information with authenticity, reliability, usability, and integrity;
- All employees share responsibility for the protection of personal information;
- Information shall be open and accessible by default and by design to the fullest extent permitted by law and subject to valid privacy and confidentiality restrictions.

4. Considerations for Security, Privacy, Records Management & Access

4.1 Security

Employees need to ensure the security of information on their devices, including City provided tokens, laptops, and mobile phones, while working remotely. The following list includes City of Toronto employee responsibilities when using Remote Access Services:

- To use the City's Secure Remote Access Service, you agree to the terms and conditions of the Secure Remote Access Use Agreement and the Acceptable Use Policy.
- You are the sole user of your token, and you must keep your token secure and PIN confidential.

- You are accountable for the security and confidentiality of files and/or data that you retrieve from the City's network. In addition, all files that you upload to the City's network must be virus-free.
- Your Secure Remote Access session is logged and is subject to management review and audit by the City of Toronto at its discretion.
- Remote Access Services are strictly for business use only.
- Any attempt to bypass the security measures that protect the City of Toronto's network is not permitted.
- If you lose your hardware token or mobile device, you must report it immediately to the Technology Service Desk or Divisional IT.

Security tips when working from home or in a public place:

- Use a secure connection rather than a public WiFi connection.
- Use privacy screens to protect your information.
- Be hypervigilant to cyberattacks, ransomware and phishing emails. Report phishing scams if you suspect them. For more information see: Avoid Phishing Scams & How to avoid a phishing attack
- Protect your devices from unauthorized access by locking the screen and storing them securely when not in use.

4.2 Privacy

Working remotely introduces new challenges in terms of protecting personal and confidential information, and staff must be aware of these challenges and take appropriate measures to reduce the level of risk.

Records and information, including e-mail exchanges, files on the shared drive, in the cloud, or on a USB, and records of telephone conversations that are business-related, are subject to MFIPPA, allowing members of the public to access them through Freedom of Information (FOI) requests. These records may contain personal or confidential information and must be protected at all times. When handling records with personal information, staff must ensure that the personal information is kept secure, and cannot be disclosed to anyone except under specific circumstances outlined in MFIPPA.

In addition, personal and confidential information must not be made available to any unauthorized individuals or third parties. Personal and confidential information, including intellectual property, must not be exposed to any risk of a potential data breach or misuse while working remotely.

The Protection of Privacy Policy provides further information on employee responsibilities to protect personal information.

Tips to ensure privacy protection:

- Use a City-approved device where possible to work remotely. Log in to the device using City-approved procedures such as VPN and remote tokens.
- If you have to use a personal device for remote work, ensure that you are following the procedures established by the Technology Services Division.
- Do not share log-in information or leave log-in information in a place where it can be accessed by someone other than yourself.
- While transmitting information, use the City's email system or the secure file transfer program by emailing FileTransfer@toronto.ca. Do not transmit any personal or confidential information through third-party email systems or other non-approved third party applications that are not on the City's network. Some examples of third party email systems are Gmail, Hotmail, Google Drive, and Dropbox.
- Avoid downloading confidential or personal information onto your computer's hard drive. If you must do so, remember to delete the information after use by:
  - deleting the file from the location you saved the record in; and
  - deleting it from the recycle bin on your desktop.
- Do not copy confidential or personal information onto USB drives since they are easily lost or stolen. If you must do so, ensure your USB drive is encrypted and delete the information after use.

Email

- Use the City of Toronto's corporate email system, Outlook, to communicate via VPN. Avoid using personal email addresses, especially if the email contains personal or confidential information;
- Ensure you have recipient(s) appropriately placed in the carbon copy (cc) and/or blind carbon copy (bcc) fields, as inappropriately listing recipients in the to or cc fields could result in a privacy breach
- Use up-to-date mailing lists
- Be aware of "phishing" emails – these are emails that originate from outside of the City but are designed to look as if they are from a legitimate source. The links may contain viruses, or may lead to a breach of personal information.
- Ensure that no personal or confidential information is being sent to unauthorized recipients.

See the Secure Use of E-mail Guideline for more information:
http://insideto.toronto.ca/clerks/policies/files/secure-use-email.pdf

External or Third Party Applications

Working remotely may require a change to many business processes. With more City services becoming available online, there will be increased use of technology which may include the use of external or third party applications. The City must take precautions prior to the use of any non-approved external or third party service, application, or technology ensuring both compliance with MFIPPA and that all personal and confidential information remains secure.

Staff may contact a Client Relationship Management (CRM) Representative to discuss approved technology options available to ensure compliance with the City's Acceptable Use of Information Technology Assets Policy and the IT Asset Management Policy. A formal consultation may be required with Risk Management & Security Services to ensure the external service, technology, or software being used is secure by conducting a risk and cyber security assessment.

Privacy Breach Management

A privacy breach is the improper collection, use, disclosure, or destruction of personal information or personal health information, according to the privacy provisions of the Municipal Freedom of Information and Protection of Privacy Act and the Personal Health Information Protection Act (the Acts).

The most common privacy breach is the unauthorized disclosure of personal information contrary to sections 32/31 of the Acts, which establish privacy regulations on the use and disclosure of personal information. Other types of privacy breaches may include a lost or misplaced file, lost or stolen mobile devices, unauthorized access to personal information/personal health information through email and other channels, or the inadvertent disclosure of that information.

How can I report a privacy breach?

If you suspect or experience any unauthorized access or disclosure, immediately report it to your manager who will initiate the Privacy Breach Management process and report it to the City's Privacy team at: privacy@toronto.ca

Staff can review the City's Privacy Breach Management procedure for more information here.

4.3 Records Management

Information created or collected remotely must be managed appropriately in order to uphold the City's recordkeeping obligations and ensure efficient continuity of City services. Information that is accurate, useable, and accessible supports an open,

transparent, and accountable local government, improving customer interactions and program delivery.

Implementing good record-keeping practices in a remote environment will help to ensure the continued management of records throughout their lifecycle, access to information by those who need it, and compliance with the City's legislation, policies, and standards for managing information responsibly.

Duty to Document: Employees have a Duty to Document decisions and activities of business value in support of programs, services, operations, reporting, performance, accountability, and auditing purposes.

With many meetings now taking place over video and teleconferencing, it is critical to ensure meeting decisions are documented, retained, and made accessible to authorized staff within the business unit or division. It must be determined what decisions need to be documented, who is responsible for documenting and retaining the decisions, and that the documentation of decisions reflects the program needs of the division.

To capture important information during meetings:

- Assign a note taker to take attendance and capture key discussion items, action items, and decisions. The note taker should circulate their notes to other attendees after the meeting to ensure all important information was captured accurately.
- Store these meeting minutes in a business designated location e.g. business application or shared drive.

Record-Keeping: Records must continue to be safeguarded against unauthorized access, managed according to the type of information contained within (e.g. personal & sensitive information), and managed with access and lifecycle requirements in mind.

Storing City Records: City records should be stored in shared drives, business applications, or electronic documents and record systems, using appropriate classifications, folder structures, and permissions. Records should not be stored on a computer desktop or on mobile devices where they are at risk of loss.

Physical City Records: Due to the risks associated with taking physical records off of City property, such as privacy or confidentiality breaches or stolen records, it is recommended that physical records remain on City property at all times. Accessing records electronically and securely through a City VPN is preferred. Records with personal information should not be removed from the office. However should staff have no alternative but to take physical records home, they must first receive appropriate divisional authorization and take all reasonable precautions to keep the record secure during transfer and use offsite until it can be returned to a City site.

If staff have no alternative but to take physical records home, the following steps should be taken:

- Contact your CIMS Records & Information Analyst prior to retrieving any physical records from a divisional file room.
- Keep a detailed list of files removed from a City site, the employee the records are entrusted to, and when they are returned to the City site. Assign someone to administer and manage the file list and follow up with staff on the status of the physical records when needed.
- When not in use, place the files in a secure filing cabinet or drawer.
- Any records required for Freedom of Information (FOI) requests must be made available for appropriate processing.
- When transporting records, do not leave the records unattended.

Digitization of City Records: While employees may need to digitize physical records at home using scanners, it should not be considered an official digitization process with the intent to replace the physical (source) record, but rather "Convenience Digitization" as defined in the Creating and Managing Digitized Records standard.

Employees should save the physical (source) record to bring into a City location at a later time to store with corresponding physical records or to scan according to divisional processes and the requirements set out in the digitization standard.

Printing Records: It is not recommended that records are printed while working remotely. Printing City records at home can pose a risk, especially for those documents that contain sensitive or personal information. Divisions should evaluate the business need to print at home and explore other opportunities to address the needs of employees or service delivery. For example, if printing is needed for ergonomic reasons or the editing of documents, divisions can consider the use of equipment or technology to address these needs e.g. ergonomic friendly hardware or improved editing software.

Divisions may also want to consider streamlining their service workflows to include eSignatures (where applicable). See the Electronic Signatures (eSignatures) Guideline or the TECHWeb eSignature website for more information.

If there is a valid business need to print records at home, the following steps should be taken:

- Do not throw City paper records in the garbage or recycle bin.
- Keep printed documents in a secure place until you can return them to the office to place them in an appropriate disposal bin and/or digitize the record and store it electronically in a business application.

Records Disposition: Records cannot be disposed of at home either electronically or physically. Records must be retained securely until they can be safely disposed of on or

at a City network or site in accordance with an approved retention and disposition schedules. Exceptions include those records on the City network or site that are undergoing a routine disposition process or records deemed transitory that can be disposed of securely within the City's network or site.

Divisions should review this guideline with their teams and discuss how they will collect, create, manage, share, and store records while working remotely

4.4 Access

Unless there is a statutory requirement not to release information, City records should be made available to the public, the media, agencies, and other City divisions. Reasons for not releasing information are detailed in specific exemptions in MFIPPA. All City employees must continue to meet their obligations to make information available.

Freedom of Information Requests

All Divisions must be prepared to respond to Freedom of Information (FOI) requests while working remotely. This includes producing electronic records or any hard copy records that are stored onsite. Please note: FOI requests may be complex, requiring a thorough review of records from numerous business units.

Divisions should designate a staff member responsible for retrieving responsive physical records from a City location or to receive physical records onsite from the Records Centre. Corporate Information Management Services (CIMS – City Clerk's Office) staff work with the relevant divisional staff to find and produce records for review in response to a request for information.

Divisions should send scanned copies of records to the staff in the Access & Privacy Unit of CIMS unless the records cannot physically be scanned, in which case photocopies are acceptable; under no circumstances should divisions send original records to the Access and Privacy Unit. Staff from CIMS' Records Services Unit that has been approved to be on-site will facilitate the retrieval of records from file rooms or the Records Centre.

Generally, FOI requests must be answered within 30 days, although there can be an extension in certain circumstances.

Details of the role divisional staff are required to perform staff in processing FOI requests can be found in the Access and Privacy Manual (see section 5 PDF). In case of uncertainty, consult with the Access & Privacy Unit in CIMS.

Routine Disclosure

Routine Disclosure is the release of certain types of administrative and operational records by divisions without a formal Freedom of Information (FOI) request. These records may be disclosed in full or with minimal severing, keeping with the provisions of MFIPPA.

As we work remotely, routinely disclosing the appropriate information is an effective way to meet public information needs. Program managers are encouraged to be proactive in anticipating the types of information the public might want, and make it easily available by posting it online or through another channel. Divisional Routine Disclosure Plans and templates can be found here.

5. Other Information Management Resources

CIMS has a Library of Information Management resources and tools to assist staff in fulfilling their responsibilities. In addition, there are several resources and tips on the City's Intranet under the City Clerk's Office. These include the following:

- Duty to Document Fact Sheet
- Information Management Fact Sheet
- Collecting Personal Information Fact Sheet
- Understanding Notice of Collection Statements Guideline
- Responsible Record-Keeping Guideline
- Electronic Signatures (eSignatures) Guideline
- What you need to know about Transitory Records Fact Sheet
- What you need to know about Managing Emails Fact Sheet
- Secure Use of E-mail Guideline

For a full list, please see http://insideto.toronto.ca/clerks/cims/im_standards.htm

Questions?

For more information, please contact:
infomgmt@toronto.ca
Corporate Information Management Services
City Clerk's Office