Hamilton Police Service Board
Use of City of Hamilton Email Address Policy
P-032

Effective date: July 23, 2026
Reviewed:
Amended:

Applicable Legislation

Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990

City of Hamilton Computer and Technology Acceptable Use Policy (HR-15-09, IT-02)

Policy Application

1. Core Usage Rules

    a. Mandatory Business Use: Members and Staff shall use assigned City of Hamilton email addresses for all Board business communications.
    b. Professional Conduct: Emails must be used for business, and inappropriate material should not be sent, forwarded, or downloaded.
    c. Restriction on Personal Opinions: City email addresses should not be used to express personal points of view that conflict with the official position of the Board or its committees.
    d. Members and Staff shall adhere to email matters noted in the most current version of the City of Hamilton's Computer and Technology Acceptable Use Policy (currently listed as HR-15-09, IT-02 revised March 24, 2024 and attached to this policy as 'Appendix A').

2. Security and Privacy

    a. Confidentiality: Emails may contain confidential information, and unauthorized distribution is prohibited.

b. Data Protection: Users must take care with attachments from unknown senders to avoid spam or security breaches.
c. Passwords: Email passwords must not be shared.

3. Records Management and Compliance

a. Record Retention: Emails are subject to the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) requirements.
b. Email Cleanup: Users are responsible for regularly deleting transitory emails and archiving official records.

Reporting

The Executive Director shall report to the Board any privacy breaches or misuse of personal and/or business email accounts.

Corporate Human Resources Policy		Updated: March 22, 2024
Work Environment		Supersedes: Computer Acceptable Use Policy (2009-02-11)
Policy No: HR-15-09, IT-02		

Computer and Technology Acceptable Use Policy

POLICY, STATEMENT & PURPOSE	The City of Hamilton provides employees, elected officials and other authorized organizations and individuals with access to IT Resources to be used for legitimate business purposes in serving the interests of the City. These technologies are valuable tools that enable Authorized Users to effectively carry out the City's business. As such, they must be used in a responsible and appropriate manner. The purpose of this policy is to outline the City's expectations regarding the use of the City's IT Resources and set clear parameters for Authorized Users to ensure clarity surrounding the use of this corporate resource. The use of this corporate resource is not a right but a privilege and is subject to the terms of this Policy. Prior to the use of City IT Resources, all Authorized Users are required to read this Policy and acknowledge their agreement to comply with it. As well, Authorized Users are required to complete the Multi-Factor Authentication (MFA) process. Authorized Users are expected to exercise good judgment and to demonstrate a sense of responsibility and consideration of others when using the City's IT Resources. All work undertaken shall be performed in an ethical and lawful manner, demonstrating integrity and professionalism by all Users.
SCOPE	This policy applies to all Authorized Users of the City's IT Resources including but not limited to City of Hamilton employees (full-time, part- time, temporary and contract); volunteers, students, interns, staff of elected officials, and all other organizations and individuals who are authorized by the City to use IT Resources.
DEFINITIONS	The following terms referenced in this Policy are defined as: **"Authorized Users"**: includes all persons who are authorized by City of Hamilton leaders to access and use the City's IT Resources for legitimate business purposes. Authorized Users include full-time, part- time, temporary and contract); volunteers, students, interns, staff of elected officials, and all other organizations and individuals who are authorized by the City to use IT Resources.

"IT Resources": includes all:

- computer software, hardware and equipment owned or issued by the City, including desktops, laptops, tablets, notebooks, servers or smart phones;
- telephones (including IP, cellular or traditional phones), and other audio/voice devices and networks, including voicemail;
- video conferencing systems and equipment;
- scanners, printers and fax machines and peripheral devices and removable media associated with the computer (such as USB drives, CDs, DVDs, etc.);
- transmission methods and services employed by the City's computer hardware and equipment, including wired, wireless and cellular networks, whether accessed from within the City's premises or elsewhere;
- Internet and e-mail systems;
- data, information and other work products such as computer programs, databases, spreadsheets, etc., created and/or maintained in using these IT resources; and
- City related data and information that is accessed, stored, created, processed, transmitted or filed in a personal electronic device.

"Multi-Factor Authentication (MFA)": is a security method that requires the User to provide two or more verification factors to confirm their identity prior to gaining access to City IT Resources such as a computers, laptops, IT applications, online accounts, or VPN.

"Non-public Information": means information that is exempt or is potentially exempt from disclosure under the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56 or the *Personal Health Information Protection Act, 2004, S.O. 2004*, c. 3, Schedule A, or that is otherwise deemed confidential. (Refer to Policy IT-04 "Data Classification" for further information about the classification and use of City data.)

Corporate Human Resources Policy		Updated: March 22, 2024
Work Environment		Supersedes: Computer Acceptable Use Policy (2009-02-11)
Policy No: HR-15-09, IT-02		

TERMS & CONDITIONS	The following terms and conditions apply to this Policy: **1. ACCESS:** **1.1** All Authorized Users are required to verify their identity using Multi-Factor Authorization (MFA) prior to gaining access to City IT Resources such as computers, laptops, City-issued cellphones, IT applications, online accounts, or VPN. Users must contact Information Technology immediately to report suspicious activity or a compromised account at the IT Service Desk at 905-546-4357. **1.2** Access to these IT Resources enables Authorized Users to conduct City business, to perform assigned duties, to research and obtain information relevant to City business and to provide information to residents, businesses and business prospects of the City of Hamilton. **1.3** Human Resources must notify Information Technology of the termination of Authorized Users on or before the individual's termination date. This notification will be Information Technology's authorization to revoke access appropriately. **2. CITY PROPERTY:** **2.1** All files and electronic communications, including email, Internet and web content systems, created on, generated by or transmitted through the City's IT Resources are deemed to be the property of the City of Hamilton. In addition, any City related data and information that is accessed, stored, created, processed, transmitted or filed in a personal electronic device is deemed to be the property of the City of Hamilton. **2.2** The conditions set forth in subsection 2.1 may be waived if: (i) an Authorized User makes a written request outlining the reasons necessitating a waiver, and (ii) a member of the City's Information Technology management team approves the request in writing, such approval to be granted at the sole discretion of management taking into consideration the specific circumstances of each individual request.

3. MONITORING:

3.1 All Authorized Users should be aware that the City's IT Resources create activity records, including, but not limited to, every Internet site visited and every message sent.

3.2 While the City of Hamilton respects the privacy of Authorized Users, it still reserves the right to monitor use of City IT Resources, including, but not limited to, any email labeled "private". Authorized Users should be aware that they have no right of ownership or expectation of privacy with regards to their use of the City's IT Resources. The City reserves the right to implement reasonable technical and procedural measures in order to:

- ensure compliance with corporate policies and standards,
- assess system or network performance and resource usage,
- protect and maintain the security of the City's IT Resources,
- protect the City's interests in the event of a reasonable suspicion of crime or inappropriate use of City IT Resources, and
- safeguard the integrity of Authorized Users.

3.3 The City reserves the right to take action, including accessing any files, information and equipment, without notice.

4. USAGE

4.1 The City's IT Resources are corporate resources. The primary use of the IT Resources shall be for business purposes.

4.2 Use of the IT Resources for personal activities including social media (Facebook, Twitter etc.) is permitted within reasonable limits, provided it does not:

- conflict with business use or time, or
- impact negatively on other Authorized Users or on the City's IT Resources, or
- adversely affect an individual's performance or work duties and responsibilities.

Personal uses that exceed these terms, uses for profit or uses that

would otherwise violate any City policy are not permitted.

Any inappropriate, excessive or abusive usage may result in an Authorized User's access privileges being limited or revoked, and City employees may also be subject to disciplinary measures up to and including dismissal.

4.3 The City reserves the right to filter and quarantine both inbound and outbound electronic content, including but not limited to email and web content, in order to ensure the security and integrity of the IT Resources.

4.4 The City reserves the right to report any illegal violations to the appropriate authorities.

4.5 The City's existing corporate policies, including, but not limited to, the "Code of Conduct for Employees", "Harassment and Discrimination Prevention", "Personal Harassment Prevention", and "Code of Conduct for Members of Council" also apply to conduct while using the City's IT Resources.

4.6 Acceptable and appropriate usage includes, but is not limited to the following list:

- Participating in professional, work-related research
- Distributing work-related correspondence, minutes, agendas and reports
- Responding to public inquiries
- Accessing work-related on-line learning opportunities
- Creating work-related information resources
- Participating in work-related mailing lists or forums
- Communicating with staff, elected officials, and appropriate outside bodies such as other levels of government, businesses, City partners, citizen groups and residents.

4.7 Authorized Users are expected to adhere to the following:

4.7.1 Authorized Users shall not distribute outside of the City's internal network any Non-public Information, unless such distribution has been properly authorized and, where necessary, properly protected (e.g., encrypted,

password- protected). (Refer to Policy IT-04 “Data Classification” for further information)

4.7.2 Authorized Users shall not, in any way, attempt to access confidential information to which they have not been previously granted access.

4.7.3 Authorized Users shall not download or install software on any City-issued IT hardware without the prior knowledge, approval and authorization of Information Technology management. Authorized Users shall not use any software that is banned for security reasons on City-issued hardware. (See the City’s Intranet site for approved and banned software.)

4.7.4 Authorized Users shall not connect unauthorized devices (including personal or vendor laptops) to the City’s network without obtaining prior approval from Information Technology. Exception: Authorized Users may connect personal devices to public wireless networks where these are provided by the City.

4.7.5 No Authorized User shall possess a hacking or password cracking tool unless authorized in writing by the Director of Information Technology for job related reasons.

4.7.6 Authorized Users shall conduct email messaging in the same manner as they would other business correspondence, being mindful of the fact that email transmissions over the Internet are not secure and may be intercepted, and that email is subject to the provisions of the Municipal Freedom of Information and Protection of Privacy Act. Authorized Users are accountable for all email sent from their individual user name.

4.7.7 Authorized Users shall ensure that their password is changed regularly and is not shared with anyone, except within the terms of this Policy. (Refer to Policy IT-03 “Password” for further information.)

4.7.8 Authorized Users must protect sensitive information. Information which is sensitive or confidential in nature should not be stored on mobile equipment, whether City

provided or personally owned. Where it is necessary to store sensitive data on mobile equipment, the information must be encrypted. (Refer to Policy IT-04 “Data Classification” for further information)

4.7.9 Authorized Users shall not use the City’s IT Resources to run a personal business. This includes photocopying or printing flyers, advertisements, etc. for a personal business or for personal gain, or sending “for profit” messages via the Internet. Exception: Authorized Users are permitted to use any approved personal “Buy and Sell” page on the City’s Intranet site.

4.7.10 Authorized Users shall not use the City’s IT Resources for any political activities. The use of the City’s name, logo, email, file systems and all other IT Resources to support any political group, political campaign or political activity of any kind is prohibited. Authorized Users who wish to run for political office must advise their management prior to announcing their candidacy to ensure there is no conflict of interest or misuse of the City’s IT Resources. (Refer to “Council Code of Conduct” and “Employee Code of Conduct” for further information).

4.7.11 Social media sites such as Facebook and Twitter are recognized as useful tools for communicating and collaborating with the public in appropriate circumstances. Authorized Users should use these sites primarily for City business purposes as approved by the Authorized User’s management. (Refer to the Corporate Communications Social Media Policy for further information on the use of social media.)

4.7.12 Authorized Users must comply with copyright and licensing restrictions on any information which has been downloaded. Authorized Users are prohibited from engaging in activities that violate the *Copyright Act (R.S.C., 1985, c.C-42)* and any applicable copyright policies that the City may implement from time to time. Material which is viewed, copied, scanned, downloaded or saved from the Internet should be primarily related to City business.

4.7.13 Authorized Users must abide by vendor license agreements. Use of applications and/or data is subject to the vendor's license agreement and may not be reproduced in any form without permission from the vendor.

4.7.14 Authorized Users who are permitted to access the City's IT Resources remotely (e.g., from home) must follow the terms of Policy IT-08 "Remote Access". Authorized Users and are required to verify their identity using Multi-Factor Authorization (MFA) prior to gaining access to City IT Resources such as computers, laptops, City-issued cellphones, IT applications, online accounts, or VPN. Authorized Users must contact Information Technology immediately to report suspicious activity or a compromised account at the IT Service Desk at 905-546-4357.

4.7.15 Authorized Users are accountable for the security of IT Resources and City information assigned to them, whether inside or outside of the City's offices. Authorized Users are required to report any damage to, or loss of, City property covered by this Policy to Information Technology and to their management immediately. The City is not responsible for any misuse of the IT Resources. Persons found to be misusing the City's resources will be responsible for any costs or damages sustained by the City or a third party, and will be obligated to indemnify the City for any claims against the City.

4.7.16 Authorized Users are required to successfully complete security awareness training as required by Information Technology. This includes an introductory course for new Authorized Users, regular refresher courses and participating in simulated phishing campaigns.

4.7.17 Authorized Users are required to follow security and data practices provided by Information Technology to protect City information. (See the City's Intranet site for further details. Security practices may change from time to time and it is the responsibility of each Authorized User to stay up to date on same.)

4.8 Unacceptable and inappropriate usage includes, but is not limited to, the following list. The only exception is in the performance of work-related matters as approved by a member of the City's Senior Leadership Team:

4.8.1 Accessing sites or transmitting material which violates any Canadian federal or provincial law or City by-law or directive, such as defamatory, discriminatory or obscene material or sites which, in the opinion of management, are inappropriate.

4.8.2 Accessing, displaying or storing email messages, graphics or images on the City's IT Resources that are obscene, harassing or fraudulent or that are offensive and conducive to a poisoned work environment. (Inadvertently accessing an inappropriate site or receiving an email with an unacceptable attachment will not be considered a violation of this Policy. Printing, scanning, saving or forwarding inappropriate material, unless approved by the Authorized User's management, shall be considered a violation of this Policy.)

4.8.3 Distributing to members of the public, any Non-public Information such as draft reports, confidential information or information unless approved by the Authorized User's management and, where necessary, proper protection. (Refer to Policy IT-04 "Data Classification" for further information)

4.8.4 Downloading files or introducing removable media to City computers without virus scanning with an approved and up-to-date virus scanner. Authorized Users are accountable for ensuring that their virus scanning software is up-to-date.

4.8.5 Downloading or storing on the City's network servers any non-work related photo, music or video files.

4.8.6 Sending chain letters, junk mail or broadcast transmissions (i.e., sending a single message to a large number of individual email addresses) unless approved by the Authorized User's management.

4.8.7 Using the Internet to access personal email accounts, including those provided by your personal Internet Service Provider (e.g., Rogers, Cogeco, Sympatico, etc.) and web- based email systems (e.g., Hotmail, Yahoo, Gmail, etc.) from within the City's network. Note: that this restriction refers to logging on and opening mailboxes in these email systems. Authorized Users may use the City's email system to correspond with Users of any type of email system.

4.8.8 Storing games, game related data or personal web site material on any City network server.

4.8.9 Sending anonymous messages or accessing the Internet under another person's network identification.

4.8.10 Allowing others who are not Authorized Users to access and utilize the City's IT Resources.

4.8.11 Sharing City accounts or passwords with any other person, except as authorized by a member of the City's Senior Leadership Team.

4.8.12 Making unauthorized copies of copyrighted software. It is the responsibility of individual departments to ensure they obtain the appropriate software licensing.

4.8.13 Changing the configuration of the City's IT Resources without authorization from Information Technology.

4.8.14 Circumventing City computer security measures, attempting to gain access to a City system for which proper authorization has not been given, probing the security at any computer site or accessing sites or tools dedicated to computer/network hacking.

	4.8.15 Leaving City computers logged on or unlocked when leaving the workplace for any extended period.
AUDITING	Where there are reasonable grounds to suspect that an Authorized User has abused or contravened this Policy, an audit of the Authorized User's usage may be undertaken, with or without notice to the Authorized User. Usage audits of Authorized Users (other than elected officials) may be authorized by a member of the City's Senior Leadership Team. Authorization shall be in writing (email or text) with a copy to Human Resources. The audit will be conducted by Information Technology in concert with the requesting department. Usage audits of elected officials may be authorized by Council. Records required for the audit will be collected by Information Technology and provided to the auditing body authorized by Council. Usage audits of any Authorized User may be requested by law enforcement officials. In the event of such a request, records required for the audit will be collected by Information Technology and provided to law enforcement as required by law or otherwise authorized by legislation.
COMPLIANCE	Failure to comply with this Policy may result in the Authorized User's access privileges being limited or revoked and City employees may also be subject to disciplinary measures up to and including dismissal.
ADMINISTRATION	This Policy is administered by the Corporate Services Department, Information Technology Division. **CONTACT**: For more information or procedures, contact Information Technology, Corporate Services Department, IT Service Desk at 905-546-4357.

Corporate Human Resources Policy		Updated: March 22, 2024
Work Environment		Supersedes: Computer Acceptable Use Policy (2009-02-11)
Policy No: HR-15-09, IT-02		

RELATED DOCUMENTS	The following related documents are referenced in this Policy: • *Municipal Freedom of Information and Protection of Privacy Act, R.S.O.* 1990, c. M.56 • *Human Rights Code*, R.S.O. 1990, c. H.19 • *Copyright Act*, R.S., 1985, c. C-42 • *Criminal Code of Canada*, R.S., 1985, c. C-46 • IT-03 Password policy • IT-04 Data Classification policy • IT-05 User Accounts policy • IT-08 Remote Access policy • Council Code of Conduct – By-law No. 16-290 • Code of Conduct for Employees Policy • Social Media Policy
HISTORY	The following stakeholders were consulted in the revisions made to this Policy: • Corporate Policy Review Group • Information Technology • Human Resources • Legal Services • City staff from several divisions • Service Excellence sub-committee • Senior Leadership Team This replaces the Computer Acceptable Use policy approved by Council of the City of Hamilton on February 11, 2009. This Policy was updated to add terms and conditions related to Multi-Factor Authorization (MFA) on March 22, 2024.

Instant Messaging and Personal Email Accounts:
Meeting Your Access and Privacy Obligations

June 2016

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Acknowledgments

The IPC gratefully acknowledges the contributions of staff at Ontario's Ministry of Government and Consumer Services, Ryerson University and the City of London, whose suggestions and insights have informed this paper.

CONTENTS

INTRODUCTION

Staff of institutions subject to the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) or the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) have access to a wide variety of popular communications tools and services. Some employees of municipal and provincial government institutions, elected officials and political staff, including elected officials, conduct business using instant messaging tools, and personal or political party email accounts (personal email accounts), in addition to their institution-issued email accounts.

These instant messaging tools and personal email accounts create a number of record keeping and compliance challenges. Some of those challenges include:

- searching for and producing records that are responsive to access requests
- ensuring that records are retained and preserved according to the requirements set out in *FIPPA* and *MFIPPA*
- ensuring the privacy and security of personal information

Records relating to the conduct of an institution's business are subject to the access and privacy provisions of *FIPPA* and *MFIPPA*, even if they are created, sent or received through instant messaging tools, or non–institutional email accounts.

The guidelines below are designed to help you meet your administrative and legal obligations under the acts.

WHAT ARE INSTANT MESSAGING TOOLS?

Instant messaging tools allow electronic, written messages to be shared in real-time. A few examples of instant messaging tools include:

- Short Message Service (SMS) or Multimedia Message Service (MMS) text messages
- BlackBerry Messenger (including Personal Identification Number protocol or "PIN-to-PIN" communications)
- internal instant messaging systems, such as Lync
- online instant messaging applications like WhatsApp, Facebook Messenger or Google Hangouts
- any other similar application that allows for real-time, written communication

ARE INSTANT MESSAGES AND EMAILS SENT FROM OR RECEIVED IN PERSONAL EMAIL ACCOUNTS "RECORDS"?

Yes. The term "record" is defined in section 2(1) of *FIPPA* and *MFIPPA*, in part, as follows:

> "record" means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes,
>
> (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, a machine readable record, any other documentary material, regardless of physical form or characteristics, and any copy thereof, and
>
> (b) … any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution

Instant messages and emails are forms of electronic correspondence and are considered records under the acts, regardless of the tool or service used to create them.

ARE INSTANT MESSAGES AND EMAILS SENT FROM OR RECEIVED IN PERSONAL EMAIL ACCOUNTS SUBJECT TO THE ACTS?

Section 10 of *FIPPA* and section 4 of *MFIPPA* state that "every person has a right of access to a record or a part of a record in the custody or under the control of an institution" unless specific exemptions apply.

The IPC has set criteria that are used to decide if a record is in the custody or control of an institution. These go beyond the physical location of a record and involve factors such as the purpose of the record, who created it, and whether or not it relates to the institution's mandate or functions.[1]

A record does not need to be both in the custody and control of an institution, but rather one or the other.[2] Therefore, in those cases where a record is not in the custody of the institution, the question is whether it is under the institution's control. In deciding this, the IPC considers the following:

1. Do the contents of the record relate to the institution's business?
2. Could the institution reasonably expect to obtain a copy of the record on request?

1 **IPC Order MO-3281** (22 January 2016)
2 **IPC Order P-239** (5 September 1991)

Applying this approach, emails sent from or received in personal email accounts have been found to be under an institution's control for *FIPPA* and *MFIPPA* purposes.[3]

HOW CAN YOU MEET YOUR ACCESS AND PRIVACY OBLIGATIONS?

The IPC strongly recommends that institutions prohibit their staff from using instant messaging tools and personal email accounts for doing business, unless they can be set up to retain and store records automatically.[4]

However, there may be situations where an institution has a legitimate business need to use these tools or accounts. If your institution is considering using instant messaging tools, or permitting the use of personal email accounts, the following steps can help you plan for compliance with the acts.

ASSESS THE RISKS AND BENEFITS

Conduct a needs analysis to determine when the use of these tools would be appropriate or necessary, and whether the benefits outweigh the risks. This does not need to be a formal review or audit.

In some cases, there may be a legitimate business need to use instant messaging. For example, university staff may determine that they need to use instant messaging tools to communicate with students or to conduct independent research.

If it is necessary to use instant messaging tools or personal email accounts for business purposes, do a thorough review of the privacy, security and access implications.

If possible, all communications should be automatically and securely retained on your institution's digital storage. Ensure that you can search and retrieve records so that you can meet your access to information and other obligations.

Consult with your information technology staff, and records and information management staff to:

- determine the types of tools that best support your institution's communications and records management needs
- determine if records can be automatically and securely retained on your institution's digital storage

3 **IPC Order MO-3281** and **IPC Order MO-3107-F** (30 September 2014)

4 This is consistent with the recommendations made by the Information Commissioner of Canada and the Information and Privacy Commissioner for British Columbia:

Information Commissioner of Canada, "**Access to Information at Risk from Instant Messaging**," November 2013, and Office of the Information and Privacy Commissioner for British Columbia, "**Use of Personal Email Accounts for Public Business**," March 2013.

However you configure your communication tools, staff need clear guidance and training to ensure records are captured and well managed.

- ensure that the tools include search and retrieval functions to support your access to information and other obligations
- if you can, disable unauthorized software on work-issued mobile and other computing devices
- ensure that the records produced by all authorized communications tools are included in your overarching records management plans and training
- include records created through all authorized communication tools in retention schedules and general records management planning

DEVELOP AND IMPLEMENT CLEAR POLICIES

You must develop clear and consistent policies on the appropriate use of communications tools. These policies should:

- identify which instant messaging tools and email accounts are permitted for business-related communications, and clearly prohibit the use of other tools and accounts
- require staff, if they have sent or received business-related communications using unauthorized tools or accounts, to immediately, or within a reasonable time, copy records to their official or authorized email account or the institution's computer or network. This can be as simple as saving a copy to a shared drive or forwarding it to an institutional email account
- inform staff that all business-related communications are subject to disclosure and retention requirements, regardless of the tool, account or device used, and that they will have to provide a copy of all business-related communications upon request
- remind staff that when they are collecting records in response to an access to information request, they must search for and produce any relevant records from instant messaging and personal email accounts

If you think staff are not complying with your policies, you must take immediate action to preserve the records.

Remember that it is not enough to develop policies. Your institution must ensure that they are implemented. You can do this by developing clear practice and procedure guides and by providing ongoing staff training.

While it is not possible to account for every potential situation that may result in non-compliance, clear policies, training and awareness go a long way in encouraging staff to responsibly manage their records. Strong policies also help institutions deal with issues as they arise. In some situations, your institution may be required to demonstrate that it has

made its best efforts to appropriately manage its records. Policies, procedures and guidelines addressing the use of instant messaging and personal email accounts can help do this.

MONITOR AND REVIEW

Your implementation plan should address compliance over time, and should include long-term monitoring and review:

- assign someone to answer questions or concerns about your policies, procedures and practices
- include spot-checks, surveys of staff practices, or other reviews in your plans to ensure that records are being appropriately saved
- if you think staff are not complying with your policies, take immediate action to preserve the records and prevent further loss of information

You cannot evade access to information requests by using instant messaging tools or personal email accounts for business purposes.

CONCLUSION

Records relating to your institution's business that are created, sent or received through instant messaging tools, or personal email accounts, are subject to the privacy and access provisions of *FIPPA* and *MFIPPA.* The use of these tools creates significant challenges for compliance with the acts and recordkeeping requirements. The IPC recommends that all institutions prohibit the use of instant messaging tools or personal email accounts when conducting institutional business. If it is necessary to use these tools, institutions must plan for compliance by implementing appropriate policy and technical mitigation strategies.

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three Acts, the Commissioner:

- **Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction,**
- **Investigates complaints with respect to personal information held by government or health care practitioners and organizations,**
- **Conducts research into access and privacy issues,**
- **Comments on proposed government legislation and programs and**
- **Educates the public about Ontario's access and privacy laws.**

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Website: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

June 2016

SEPTEMBER 2023

INTERPRETATION

BULLETIN

Custody or Control

This interpretation bulletin outlines the factors to determine if a record is in the custody or under the control of an institution, as set out in **section 10(1)** of the *Freedom of Information and Protection of Privacy Act* and **section 4(1)** of the *Municipal Freedom of Information and Protection of Privacy Act*. This document further explains how to determine "custody or control" when an institution holds the record or when another individual or organization holds the record.

Section 10(1) of FIPPA and section 4(1) of MFIPPA read in part as follows:

"[…] every person has a right of access to a record or a part of a record in the custody or under the control of an institution unless […]".

IS THE RECORD "IN THE CUSTODY" OR "UNDER THE CONTROL" OF THE INSTITUTION?

Under section 10(1) of FIPPA and section 4(1) of MFIPPA, the right of access applies to a record that is in the custody **or** under the control of an institution; the record need not be both.[1]

If the record is not in the custody or under the control of the institution, the general right of access is not established and none of the exclusions or exemptions need to be considered.

1 Order **P-239** and ***Ministry of the Attorney General v. Information and Privacy Commissioner*, 2011 ONSC 172 (Div. Ct.)**.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

The courts and the IPC have given a broad and liberal interpretation to the concept of "custody or control"[2] consistent with the well-established principle that FIPPA and MFIPPA "shall … receive such fair, large and liberal construction and interpretation as will best ensure the attainment of the object of the *Act* according to its true intent, meaning and spirit."[3]

In deciding whether a record is in the custody or control of an institution, the factors outlined below are considered in context and in light of the purposes of the *Acts*.[4]

DETERMINING "CUSTODY OR CONTROL" WHEN AN INSTITUTION HOLDS THE RECORD

Mere possession of a record is not necessarily determinative of whether a record is in the custody or under the control of an institution. The IPC considers the following non-exhaustive list of factors when deciding if a record that is held by an institution is in the custody or under the control of that institution.[5]

- Was the record created by an officer or employee of the institution?[6]
- What use did the creator intend to make of the record?[7]
- Does the institution have a statutory power or duty to carry out the activity that resulted in the creation of the record?[8]
- Is the activity in question a "core," "central" or "basic" function of the institution?[9]
- Does the content of the record relate to the institution's mandate and functions?[10]
- Does the institution have physical possession of the record, either because its creator provided it voluntarily or pursuant to a statutory or employment requirement?[11]

---

2 ***Ontario Criminal Code Review Board v. Hale*, 1999 CanLII 3805 (ON CA)**; ***Canada Post Corp. v. Canada (Minister of Public Works)*, 1995 CanLII 3574 (FCA)**; and Order **MO-1251**.

3 ***City of Toronto Economic Development Corp. v. Ontario (Information and Privacy Commissioner)***, 2008 ONCA 366 (CanLII) at para. 30, adopted in ***Toronto Police Services Board v. (Ontario) Information and Privacy Commissioner***, 2009 ONCA 20 (CanLII) at para. 43.

4 ***City of Ottawa v. Ontario*, 2010 ONSC 6835 (Div. Ct.), leave to appeal refused (March 30, 2011), Doc. M39605 (C.A.).**

5 Orders **120**, **MO-1251**, **PO-2306** and **PO-2683**.

6 Order **120**.

7 Orders **120** and **P-239**.

8 Order **P-912**, upheld in *Ontario Criminal Code Review Board v. Hale*, cited above.

9 Order **P-912**.

10 *Ministry of the Attorney General v. Information and Privacy Commissioner*, cited above; *City of Ottawa v. Ontario*, cited above, and Orders **120** and **P-239**.

11 Orders **120** and **P-239**.

- If the institution does have possession of the record, is it more than "bare possession"? In other words, does the institution have the right to deal with the record in some way and does it have some responsibility for its care and protection?[12]
- If the institution does not have possession of the record, is it being held by an officer or employee of the institution for the purposes of their duties as an officer or employee?[13]
- Does the institution have a right to possession of the record?[14]
- Does the institution have the authority to regulate the record's content, use and disposal?[15]
- Are there any limits on the uses to which the institution may put the record?[16]
- To what extent has the institution relied on the record?[17]
- How closely is the record integrated with other records held by the institution?[18]
- What is the usual practice of the institution and institutions similar to the institution in relation to possession or control of records of this nature?[19]

This list is not exhaustive. Some of these factors may not apply in a specific case, while other factors not listed above may apply.

DETERMINING "CUSTODY OR CONTROL" WHEN ANOTHER INDIVIDUAL OR ORGANIZATION HOLDS THE RECORD

The Supreme Court of Canada has adopted the following two-part test to determine whether an institution has control of records that are not in its physical possession:

(1) Do the contents of the document relate to a departmental matter?

(2) Could the government institution reasonably expect to obtain a copy of the document upon request?[20]

---

12 Order **P-239** and *Ministry of the Attorney General v. Information and Privacy Commissioner*, cited above.

13 Orders **120** and **P-239**.

14 Orders **120** and **P-239**.

15 Orders **120** and **P-239**.

16 *Ministry of the Attorney General v. Information and Privacy Commissioner*, cited above; Order **MO-2586**.

17 *Ministry of the Attorney General v. Information and Privacy Commissioner*, cited above, and Orders **120** and **P-239**.

18 Orders **120** and **P-239**.

19 Order **MO-1251**; Order **MO-2586**.

20 ***Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2011 SCC 25 (CanLII), [2011] 2 SCR 306**.

In addition, the following factors may also be relevant in determining whether a record is in the custody or under the control of an institution even when another individual or organization holds the record:

- If the record is not in the physical possession of the institution, who has possession of the record, and why?[21]
- Is the individual, agency or group who has physical possession of the record an "institution" for the purposes of the *Act*?[22]
- Who owns the record?[23]
- Who paid for the creation of the record?[24]
- What are the circumstances surrounding the creation, use and retention of the record?[25]
- Are there any contractual provisions between the institution and the individual who created the record that give the institution the express or implied right to possess or otherwise control the record?[26]
- Was there any understanding or agreement between the institution and the individual who created the record or any other party that the record was not to be disclosed to the institution? If so, what was the precise undertaking of confidentiality given by the individual who created the record, to whom was it given, when, why and in what form?[27]
- Is there any other contract, practice, procedure or circumstance that affects the control, retention or disposal of the record by the institution?[28]
- Was the individual who created the record an agent of the institution for the purposes of the activity in question? If so, what is the scope of that agency, and does it carry with it a right of the institution to possess or otherwise control the records? Did the agent have the authority to bind the institution?[29]
- To what extent did the institution rely or intend to rely on the records?[30]

---

21 Order **PO-2683**; Order **MO-2586**.

22 Order **MO-2586**.

23 Order **M-315**.

24 Order **M-506**.

25 Order **PO-2386**.

26 ***Greater Vancouver Mental Health Service Society v. British Columbia (Information and Privacy Commissioner)*,1999 CanLII 6922 (BC SC)**; Order **MO-1251**; Order **MO-2586**.

27 Orders **M-165** and **MO-2586**.

28 Order **MO-2586**.

29 ***Walmsley v. Ontario (Attorney General)* (1997), 34 O.R. (3d) 611 (C.A.)** and ***David v. Ontario (Information and Privacy Commissioner) et al* (2006), 217 O.A.C. 112 (Div. Ct.).**; Order **MO-1251**; Order **MO-2586**.

30 Order **MO-1251**.

- What is the customary practice of the individual who created the record and others in a similar trade, calling or profession, to possess or control records of this nature in similar circumstances?[31]
- Does the institution have a statutory power or duty to carry out the activity which resulted in the creation of the records, and is the activity in question a "core", "central" or "basic" function of the institution?[32]

31 Order **MO-1251**; Order **MO-2586**.

32 Order **MO-1251**.

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario