

Bill No. 548
2018

By-law No. CPOL.-____-____

A by-law to adopt a new Council policy entitled
“Access and Privacy Policy”.

WHEREAS section 5(3) of the *Municipal Act, 2001*, S.O. 2001, C.25, as amended, provides that a municipal power shall be exercised by by-law;

AND WHEREAS section 9 of the *Municipal Act, 2001*, S.O. 2001, C.25, as amended, provides a municipality with the capacity, rights, powers and privileges of a natural person for the purpose of exercising its authority;

AND WHEREAS the Council of The Corporation of the City of London wishes to adopt a new Council policy entitled “Access and Privacy Policy”;

NOW THEREFORE the Municipal Council of The Corporation of the City of London enacts as follows:

1. The Policy entitled “Access and Privacy Policy” attached as Schedule “A” is hereby adopted.
2. This by-law shall come into force and effect on the date it is passed.

PASSED in Open Council on September 18, 2018.

Matt Brown
Mayor

Catharine Saunders
City Clerk

First Reading – September 18, 2018
Second Reading – September 18, 2018
Third Reading – September 18, 2018

SCHEDULE "A"

Policy Name: Access and Privacy Policy

Legislative History: None

Last Review Date: August 15, 2018

Service Area Lead: Manager, Records and Information Services

1. Policy Statement

The Access and Privacy Policy is a general guide to the *Municipal Freedom of Information and Protection of Privacy Act* ("MFIPPA" or "Act").

The policy combines current practice and procedures and offers operational guidance to help staff:

- Understand the general framework of the legislation;
- Meet administrative and operational requirements; and
- Be aware of best practices.

The policy is not meant to provide legal advice. This policy should be referenced in conjunction with an up-to-date version of the legislation and regulations.

2. Definitions

Please refer to Section 2 of the attached Appendix "A".

3. Applicability

This policy applies to all City of London employees and governs the procedure by which City of London employees respond to Freedom of Information requests and protect personal information as required under MFIPPA.

4. The Policy

Please refer to the attached Appendix "A"

“APPENDIX “A”

Access and Privacy Policy

TABLE OF CONTENTS

1. Purpose and Policy Statement.....	3
Audience.....	3
Policy Principles	3
Transparency.....	3
Accountability.....	3
2. Definitions.....	4
3. Roles and Responsibilities.....	6
The Head.....	6
City Manager and Service Area Leads.....	6
City of London Employees.....	6
Service Area Liaisons.....	7
Legal & Corporate Services – City Solicitor’s Office.....	7
4. Timely Response to Access Requests	7
Follow-up Process.....	8
5. Access Request Procedures	8
Receiving Requests.....	8
Clarifying Requests.....	8
Access Procedure	8
Time Extensions.....	9
Providing Records to the Head	10
Offence	10
Reviewing and Disclosing Records.....	10
Fees.....	11
6. Councillors’ Records.....	12
7. Access to Records of Personal Health Information	13
8. Appeals to the Information and Privacy Commissioner (IPC)	13
Offence.....	13
9. Personal Information.....	14
Protection of Personal Privacy.....	14
Collection of Personal Information.....	14
Retention of Personal Information.....	14
Use of Personal Information.....	14
Offence.....	15

Privacy Investigations.....15

10. Protocol for Responding to a Privacy Breach Under the act.....16

 Containment:.....16

 Notification:.....16

11. Appendices.....16

 Appendix A – MFIPPA PROCESS MAP17

 Appendix B – RECORDS RETRIEVAL FORM.....18

Access and Privacy Policy

A policy governing the procedure by which City of London employees respond to Freedom of Information requests and protect personal information as required under the *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990 ("MFIPPA" or "Act").

1. PURPOSE AND POLICY STATEMENT

The Access and Privacy Policy is a general guide to MFIPPA.

The policy combines current practice and procedures and offers operational guidance to help staff:

- Understand the general framework of the legislation;
- Meet administrative and operational requirements; and
- Be aware of best practices.

The policy is not meant to provide legal advice. This policy should be referenced in conjunction with an up-to-date version of the legislation and regulations.

Audience

The primary audience for this policy is City of London staff.

Policy Principles

The following principles will form the basis of this policy:

Transparency

- As identified in the Strategic Plan, the promotion of an open and transparent government is important to the City of London.
- The City of London is committed to both the routine disclosure and the active dissemination of records when consistent with the principles and rules of the Act.
- The City of London will provide access to records and information in accordance with the principles and rules of the Act.

Accountability

- The City of London will take reasonable steps to protect the collection, use, and disclosure of personal information.
- The City of London will facilitate an individual's right of access as well as the ability to correct his or her personal information in the custody or under the control of the institution, subject to any legislative exemptions.

2. DEFINITIONS

The terms that appear below are referenced from the Act and relevant IPC guidance documents and Orders.

"Custodian" person or organization within the meaning of the *Personal Health Information Protection Act, 2004* ("PHIPA") that, as a result of his, her or its power or duties or work set out in PHIPA, has custody or control of personal health information.

"Experienced Employee" (IPC Order PO-3423), employees who were knowledgeable in the subject matter of the request and expend a reasonable effort to locate responsive records.

"Head" in respect of an institution, the individual or body determined to be head under section 3 of the Act.

"Information and Privacy Commissioner" and **"IPC"** mean the Commissioner appointed under subsection 4 (1) of the *Freedom of Information and Protection of Privacy Act*.

"Institution" (section 2 of the Act),

- (a) a municipality,
- (b) a school board, municipal service board, city board, transit commission, public library board, board of health, police services board, conservation authority, district social services administration board, local services board, planning board, local roads board, police village or joint committee of management or joint board of management established under the *Municipal Act, 2001* or the *City of Toronto Act, 2006* or a predecessor of those Acts,
- (c) any agency, board, commission, corporation or other body designated as an institution in the regulations; ("institution").

"Personal Information" recorded information about an identifiable individual, including,

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual;
- (b) 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;
- (c) any identifying number, symbol or other particular assigned to the individual;
- (d) the address, telephone number, fingerprints or blood type of the individual;
- (e) the personal opinions or views of the individual except if they relate to another individual;
- (f) 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;
- (g) the views or opinions of another individual about the individual; and
- (h) 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.

"Personal Health Information" (section 4 of PHIPA), identifying information about an individual in oral or recorded form, if the information,

- (a) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;
- (b) relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;
- (c) is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual;
- (d) relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual;
- (e) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance;
- (f) is the individual's health number; or
- (g) identifies an individual's substitute decision-maker.

"Privacy Breach"

- (a) A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the Act. Among the most common privacy breaches is the unauthorized disclosure of personal information, contrary to section 32 of the Act. For example, personal information may be lost (a file is misplaced within an institution), stolen or inadvertently disclosed through human error (a letter addressed to person A is actually mailed to person B).

"Record" (section 2 of the Act), 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, an email, [an instant/text message](#), 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.

"Responsive Record" (IPC Order PO-2554), any record that reasonably relates to, or is within the scope of a request under the Act.

"Reasonable Search" (IPC Order M-909 and [IPC Fact Sheet](#)), a search conducted by an experienced employee expending reasonable effort to identify any records that are reasonably related to the access request in locations where records in question might reasonably be located.

"Service Area Liaison" as designated by their Managing Director or designate, a City of London employee with sufficient experience and training in MFIPPA access processes and procedures who responds to the Head with respect to routine access requests on behalf of their department.

3. ROLES AND RESPONSIBILITIES

The Head

The Act prescribes Council as the Head of the Institution for the purposes of the Act. As Head, Council is accountable for decisions under the Act and for overseeing how the City administers the Act generally. This responsibility includes complying with access provisions of the Act, and ensuring that personal information that the institution collects, uses, and discloses is in compliance with the Act. Pursuant to section 49 of the Act, City Council has delegated to the City Clerk its powers and duties under the Act as per [By-law No. A.-6067-31](#).

For the purposes of this policy, the City Clerk or designate is responsible for:

- exercising the duties pursuant to Council's delegation of all its powers and duties as Head and properly discharging its statutory obligations pursuant to section 49(1) of the Act;
- receiving and managing the overall process of responding to access requests under the Act;
- communicating and liaising with staff, requesters, and third parties regarding access requests under the Act;
- preparing records for disclosure and determining access to records subject to the provisions of the Act;
- managing all aspects of the appeal process relating to access requests under the Act;
- communicating with Managing Directors and/or City Manager to resolve any delays by division staff in searching, retrieving or providing copies of records responsive to access requests under the Act;
- preparing and submitting the annual report to the IPC;
- providing training to employees on the Act; and
- administering, monitoring, and promoting all aspects of this policy.

City Manager and Service Area Leads

The City Manager (generally) and each Service Area Lead (with regards to his or her direct reports) is responsible for ensuring that the employees they oversee adhere to the procedures in this policy and the provisions of the Act.

The City Manager and Service Area Leads are responsible for:

- allocating sufficient employees and other resources to ensure that Service Areas comply with the access and privacy requirements of the Act;
- ensuring that employees meet internal and statutory deadlines for responding to access requests;
- ensuring that employees maintain division records in compliance with management policies and procedures, and the City of London's Records Retention By-law; and,
- appointing an employee to act as a Service Area Liaison between the respective Service Area and the Head.

City of London Employees

All City of London employees shall be aware of and comply with this policy as required and shall also be responsible for:

- maintaining records in compliance with management policies and procedures and the City of London's Records Retention bylaw;
- locating, retrieving and providing copies of records to the Head in response to a request made under the Act by the deadlines provided;
- participating in MFIPPA and records management training;
- communicating and cooperating with the Head with respect to requests made under the Act (for example, search time estimates, clarification requirements, concerns with records, etc.); and,
- providing the Head with a completed Records Retrieval Form (**Appendix B**).

Service Area Liaisons

Each Service Area (SA) shall appoint an employee to act as the SA Liaison between the SA and the Head in response to MFIPPA requests SA Liaisons will receive specialized training by the Head and shall be responsible for fulfilling the access request procedures set out within this policy.

Legal & Corporate Services – City Solicitor's Office

Solicitors in the City Solicitor's Office provide legal advice to the Head on access requests, as required. Solicitors in the City Solicitor's Office shall be responsible for:

- providing legal advice and opinions related to requests under the Act;
- representing (as required by the Head) the City on appeals to the IPC of the Head's decisions under the Act and in proceedings before the IPC; and,
- preparing representations or reconsideration requests, when requested by the Head, regarding inquiries conducted by the IPC in accordance with the timelines set by the IPC.

4. TIMELY RESPONSE TO ACCESS REQUESTS

The Head is legislatively required to respond to MFIPPA requests within 30 calendar days. Accordingly, requests are processed within 20 - 21 *business* days.

If the Head does not respond to a request within the 30 day time period, then the request is deemed to have been refused. The Act then entitles requesters to appeal immediately the "deemed refusal" to the IPC.

Because of the legislated time frames, employees should process MFIPPA requests on a priority basis. The Head will send a department letter requesting records directly to the SA Liaison with a specific deadline for the responsive records to be provided to the Head. Generally, 13-15 calendar days are allocated for staff to complete the search and provide copies of responsive records to the Head.

Search time estimates which exceed one (1) hour are to be provided to the Head with three (3) days of receipt of the department letter. If no search time estimate is received by the Head, the expectation is that the SA Liaison will provide responsive records by the due date indicated in the department letter.

Follow-up Process

If the SA Liaison has not provided the Head with a search time estimate and the Head has not received responsive records by the due date, the Head will follow-up as follows:

- Day Records are Due – Reminder to SA Liaison that records are due today;
- 2 Days After Due Date – If no response, a second reminder to the SA Liaison;
- 4 Days After Due Date– If no response, communication sent to the Managing Director advising that the division response is overdue and that, if the responsive records are not received in the next few days, the request will become overdue;
- 6 Days After Due Date – If no response, communication sent to the City Manager advising that the division response is overdue and that, if the responsive records are not received, the request will become overdue.

5. ACCESS REQUEST PROCEDURES

Receiving Requests

The Head will seek to determine whether a requester may obtain access to all or some of the requested records directly from the relevant Service Area; for example, by providing information that is public. Service Areas should advise the Head of any circumstances when they can routinely disclose certain records outside of the formal freedom of information access procedure.

The Head processes all other formal requests for access to records under the Act.

Clarifying Requests

The Head will seek to ensure that requests are as clear as possible and will contact the requester where appropriate to seek clarification.

Access Procedure

Refer to Process Map – [Appendix A](#)

1. Once the Head has clarified a request, a department letter, a copy of the request, and Records Retrieval Form is prepared and sent to the SA Liaison with a copy to the Managing Director.
2. Requests that require searches of the Microsoft Exchange system are forwarded directly to the Director of IT, Finance & Corporate Services. Results are provided directly to the Head. The Head will provide copies of responsive e-mails to the staff member for their review.
3. The SA Liaison may identify other Service Areas that may have responsive records.
4. SA Liaisons are required to notify the Head within three (3) days of receipt of the department letter if they anticipate a search for responsive records will take more than one (1) hour. If the search is anticipated to take an hour or less, SA Liaisons are advised to provide copies of records (either electronically or photocopies) by the deadline provided in the letter.

5. SA Liaisons must search for all recorded information that responds to an access request and provide copies of the records to the Head no later than the return date indicated in the letter. A search for responsive electronic records can be done through keyword search or reviewing responsive content folders. A search for paper records can be done by physically looking in cabinets or boxes.

If SA Liaisons require a time extension to complete a search they should contact the Head immediately to determine whether the Act permits a time extension. SA Liaisons are required to prepare documentation to justify search time estimates and requests for time extensions, if applicable. Please see the "Time Extensions" section below for detailed documentation requirements.

6. The Head requires that SA Liaisons return a completed Records Retrieval Form along with responsive records indicating the actual time spent searching for records, the location and methods used to search for records, and/or whether there are any concerns with the records in question. The Head also requires a completed Records Retrieval Form if no records are provided responsive to the request.

In the event of an appeal, the IPC may call on the staff that searched for the records to describe the steps they took to conduct the search. Referencing the Records Retrieval Form in such instances assists the Head during the appeal process.

7. The Head will, at the request of the SA Liaison or Managing Director, advise when the records pertaining to their business unit will be released. Where legislative timelines permit, the Head will, at the request of the SA Liaison or Managing Director, provide copies of the records to be released prior to their release.

Time Extensions

The Head determines extensions for a request based on input from the SA Liaison and/or the Service Area Managing Director.

The Act allows the Head to extend the processing time for a request when:

1. The request is for a large number of records or necessitates searching through a large number of records and meeting the time limit would unreasonably interfere with the operations of the City; or
2. Staff must consult with an external agent to comply with the request and they cannot reasonably complete the consultation within the time limit.

If either of the above factors apply, the SA Liaison should summarize in writing the reasons for an extension as follows:

a) For a request involving a large numbers of records by:

- explaining the steps that employees require to search for responsive records and estimating the total number of pages of records;
- identifying any exemptions that may be applicable to the records; and,
- providing a representative sample of records.

b) For a request that cannot be completed without consulting with an external agent person, by

providing:

- the name of the person or organization that the City will consult;
- the reason why consultation is necessary; and,
- an estimate about when the consultation will be complete.

Providing Records to the Head

The SA Liaison shall provide all of the responsive records to the Head (by the deadline) using the following guidelines:

- Records (electronic or paper) must be provided unaltered. The Head will not accept records that have been redacted or "blacked-out".
- Original paper records are to be copied. Copies must be legible.
- Electronic records should be provided via the City of London's Internal File Transfer Service or provided on an ITS approved USB stick. Please do not print electronic records.
- The SA Liaison should identify any areas of concerns in any of the responsive records and may, solely for the purpose of assisting the Head, identify any exemptions that the liaison believes may apply to the records noting that the final decision rests with the Head.
- A completed Records Retrieval Form must be submitted with the records by the deadline.

Offence

No employee shall alter, conceal or destroy a record or cause another person to do so with the intention of denying a right under the Act to access the record or the information contained in the record.

It is an offence under section 48(1)(c.1) of the Act to alter, conceal or destroy a record, or cause any other person to do so, with the intention of denying a right under the Act to access the record or the information contained in the record. Every person who contravenes subsection (1) is guilty of an offence and on conviction is liable to a fine not exceeding \$5,000.00.

Reviewing and Disclosing Records

The Act requires that the Head must disclose as much of the requested record as can reasonably be severed, without disclosing the information that falls under one of the exemptions. Severing is the process of "blacking out" or "redacting" information that is considered confidential and exempt from disclosure.

Only the Head will sever records responsive to a formal access request under the Act. Severances are decisions on disclosure, and the Head is the only decision-maker at the City of London who has the authority to make decisions on disclosure under the Act.

To assist the Head in determining whether a record is exempt from access or outside the scope of the Act the Head will consider recommendations of the SA Liaison. Any such recommendations should be recorded on the Records Retrieval Form.

When the Head refuses access to a record or severs part of a record, the Act requires the Head to provide the requester with a decision letter that:

- explains the basis for the decision;
- describes clearly to the requester the records responding to the request specifically referring to the exemption(s) that the City has applied to justify a refusal to provide access;
- may include a detailed index of records that describes the contents and subject matter of the records;
- notifies the requester if the requested record does not exist; and,
- states that the requester may appeal the Head's decision to the IPC.

If a request is received for records that appear to be excluded from the Act, the Head will process the request in accordance with the procedure set out in this policy.

Fees

For all requests under MFIPPA, the requester must pay a \$5.00 application fee. The application fee is mandatory and the Head cannot waive it.

The Head applies different fees as prescribed by regulation, depending on whether the request is for *general records* or for the requester's own personal information.

The Head must charge fees unless the Head decides to waive the fees under the fee-waiver provisions of the Act.

The regulations under the Act contain a fee schedule that sets out the amount that the Head may charge for various costs that the City may incur when processing a request:

Type of Fee	Amount
Application Fee	\$5.00
Photocopies and computer printouts	\$0.20 cents per page
Disks	\$10.00 per disk
Manual search for records *	\$7.50 for each 15 minutes spent
Preparing a record for disclosure, including severing records *	\$7.50 for each 15 minutes spent
Computer programming	\$15.00 for each 15 minutes spent
Costs incurred in locating, retrieving, processing and copying the record	As specified in an invoice received by the City

* does not apply to a request from an individual for their own personal information.

6. COUNCILLORS' RECORDS

The Head will determine whether the Act applies to a councillor's records. In making this decision, the Head examines the specifics of each request in light of a number of [principles established by the IPC](#).

Councillors' records are subject to the Act where:

- (a) a councillor is acting as an officer or employee of the municipality, or performs a duty assigned by council, such that they might be considered part of the institution, or,
- (b) the records are in the custody or control of the municipality on the basis of established principles.

The access procedure for requests related to Councillors' records shall follow the standard procedure described within this policy.

1. Once the Head has clarified a request, a department letter, a copy of the request, and Records Retrieval Form is prepared and sent to the Executive Assistant (EA) to the Councillors' Office, or designate.
2. If the search requires electronic communications, the Councillor may request a search of their Microsoft Exchange account to be completed by the Information and Technology Services Department. Results will be provided directly to the Head. The Head will provide copies of responsive e-mails to the Councillor for their review.
3. Councillors (or the EA) are required to notify the Head within three (3) days of receipt of the department letter if they anticipate their search for responsive records will take more than one (1) hour. If the search is anticipated to take an hour or less, Councillors (or the EA) are advised to provide copies of records (either electronically or photocopies) by the deadline provided in the letter.
4. Councillors (or the EA) must retrieve and provide copies of the records to the Head no later than the due date indicated in the letter. If Councillors require a time extension to complete a search they should contact the Head immediately to determine whether the Act permits a time extension.
5. The Head requires that Councillors (or the EA) return a completed Records Retrieval Form along with responsive records which indicates the actual time spent searching for records, the location and methods used to search for records, whether there are any concerns with the records in questions, etc. The Head also requires a completed Records Retrieval Form if no records are provided responsive to the request.
6. The Head will, at the request of the Councillor, advise when the records pertaining to them will be released and/or provide copies of the records to be released prior to their release.

7. ACCESS TO RECORDS OF PERSONAL HEALTH INFORMATION

An individual may exercise a right of access to a record of personal health information by making a written request for access to the custodian that has custody or control of the information.

Organizations that are both *custodians* under PHIPA and *institutions* under the Act include municipally operated long-term care homes, for example, Dearness Home.

The Head will determine whether PHIPA or MFIPPA applies to a request it receives having regard to the legislation.

If the Head receives a request for personal health information in the custody or under the control of Dearness Home, the Head will immediately transfer that request to the Administrator of Dearness and advise the requester of the same.

If the Administrator of Dearness receives a request under the Act for information in the custody or under the control of the City of London, the Administrator will immediately transfer that request to the Head and advise the requester of the same.

8. APPEALS TO THE INFORMATION AND PRIVACY COMMISSIONER (IPC)

The Act establishes the right of a requester to appeal decisions that the Head makes about access to records. After a requester receives a notice of decision, the requester has 30 calendar days to appeal the decision to the IPC.

The Head, in consultation with the City Solicitor's Office, will respond to appeals as per the procedures and practice directions set out in the IPC's [Code of Procedure for appeals under the Freedom of Information Act and the Municipal Freedom of Information and Protection of Privacy Act](#), (hereafter "Code of Procedure").

The Head will notify the appropriate staff member (or Councillor) and the appropriate Managing Director, in the event that the Commissioner issues an order with respect to access to records. The Head will ensure compliance of the order.

The Head will notify the City Manager and the appropriate Managing Director should the IPC notify the head that the Commissioner will be entering and inspecting any premise occupied by The City of London for the purposes of an investigation. The Head will be in attendance during the IPC's inspection.

Offence

No employee shall wilfully obstruct the IPC in the performance of its functions, make a false statement to mislead the IPC or fail to comply with an order of the IPC.

Any person who wilfully obstructs the IPC in the performance of its functions, makes a false statement to mislead the IPC, or fails to comply with an order of the IPC, is guilty of an offence, and on conviction, is liable to a fine of up to \$5,000.00.

9. PERSONAL INFORMATION

Protection of Personal Privacy

The Act requires that the Head implement basic standards for protecting personal information in its possession. Refer to the [IPC'S Fact Sheet](#) to learn more about how *Personal Information* is defined in the Act.

Collection of Personal Information

The City, employees or consultants acting on the City's behalf, shall only collect personal information that they are authorized to collect. This authority can be one of the following:

- collection of the information is expressly authorized by provincial or federal legislation;
- the information is used for the purposes of law enforcement; or,
- the information is necessary to the proper administration of a lawfully authorized activity.

The City shall only collect personal information directly from the individual to whom it relates, except in circumstances set out in MFIPPA. Examples of these include:

- where the individual authorizes another method of collection;
- the personal information may be disclosed to the City under the authority of the Freedom of Information and Protection of Privacy Act ("FIPPA");
- where the IPC has authorized the City to collect the information indirectly from another person;
- the information is collected for the purpose of law enforcement; and,
- where other legislation provides for a different method of collection.

When collecting personal information, the City must provide the individual with a [notice of collection](#) statement that contains:

- the City's legal authority to collect the information;
- the principal purposes for which the information is intended to be used; and,
- the title, business address and telephone number of an officer or employee who can answer questions about the collection (why it is being collected, how it will be used).

Notice of collection statements are prepared by staff in consultation with the Head. Exceptions to this notice requirement are set out in O. Reg. 823.

Retention of Personal Information

Personal information that has been collected by the City must be retained for at least one year after it is used, unless another retention period has been provided in the City's Records Retention by-law, or the individual has consented to its earlier disposal. The purpose of this retention period is to ensure that individuals have a reasonable opportunity to obtain access to their personal information.

Use of Personal Information

The City is required to take reasonable steps to ensure that personal information is not used unless it is accurate and up to date. The City must create a record of any use of personal

information that is different from how the information is used on a regular basis.

The City is only permitted to use personal information:

- if the individual has consented to the particular information being used;
- for the purpose for which it was obtained or compiled;
- for a consistent purpose, (i.e. the individual might reasonably expect the use); or
- for the purpose for which the information was disclosed to the City under FIPPA.

Disclosure of Personal Information

The City is only permitted to disclose personal information in the following circumstances:

- in compliance with Part I of the Act;
- if the individual has consented to its disclosure;
- for the purpose for which it was obtained;
- for a consistent purpose, (i.e. the individual might reasonably expect the disclosure);
- disclosure is made to an employee who needs the record in the performance of duties;
- to comply with federal or provincial legislation;
- to a law enforcement agency in Canada to aid an investigation;
- in compelling circumstances affecting personal health or safety;
- in compassionate circumstances, (to contact next of kin or friend of an injured, ill or deceased person); and,
- to a provincial or federal government department for auditing of cost-shared programs.

Offence

Any person who wilfully discloses personal information, or maintains a personal information bank, in contravention of the Act, is guilty of an offence, and on conviction, is liable to a fine of up to \$5,000.00.

Privacy Investigations

Individuals may submit a complaint to the IPC if they believe that the City of London has improperly collected, used, disclosed, retained or disposed of their personal information.

The Head shall receive notice from the IPC in the event that an individual has lodged a complaint and an investigation is being undertaken.

The Head shall, in consultation with appropriate staff, represent the institution during a privacy complaint investigation.

The responsible employee will cooperate and assist the Head during the course of the investigation.

10. PROTOCOL FOR RESPONDING TO A PRIVACY BREACH UNDER THE ACT

Upon learning of a privacy breach or a potential privacy breach under MFIPPA, staff shall immediately notify their Manager and the Head.

The Head will assist the responsible employee in responding to the breach of personal privacy.

The following protocol shall be adopted during a breach or a potential breach of personal privacy, as per [IPC guidelines](#).

Containment: Identify the scope of the breach or potential breach and take steps to contain it:

- retrieve hard copies of any personal information that has been disclosed;
- ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that follow-up is required; and,
- determine whether the privacy breach would allow unauthorized access to any other personal information (i.e. financial institutions).

Notification: Identify those individuals whose privacy was breached and, barring exceptional circumstances, in consultation with the Head, notify those individuals accordingly:

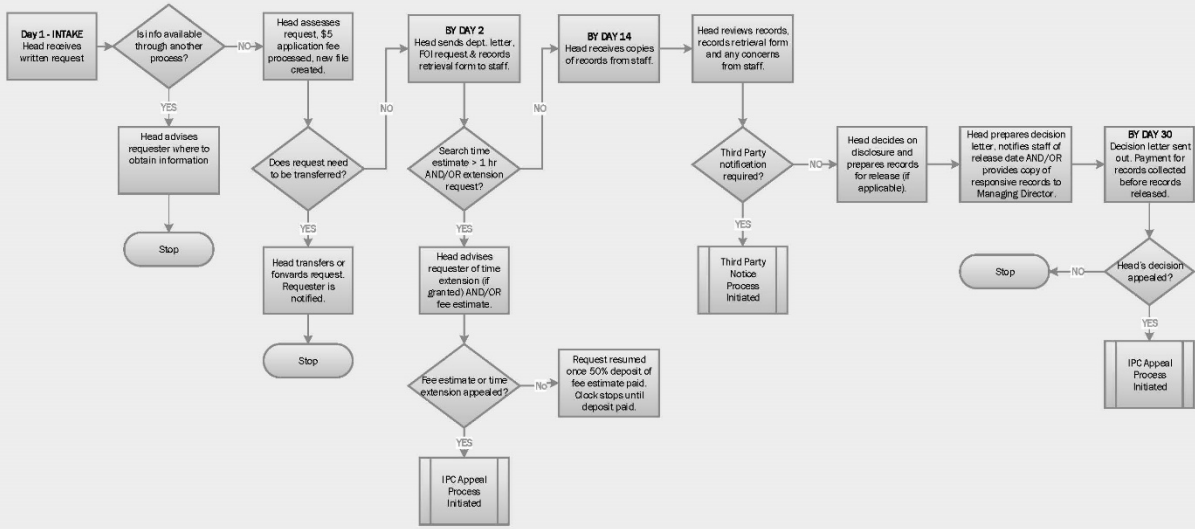
- notify the individuals whose privacy was breached, by telephone or in writing;
- provide details of the extent of the breach and the specifics of the personal information at issue;
- if financial information or information from government-issued documents are involved, include precautionary measures in the notice, (i.e. change passwords, contact Equifax or banking institution, etc.);
- advise of the steps that have been taken to address the breach, both immediate and long term;
- provide contact information for someone who can provide additional information, assistance and answer questions; and,
- advise if the IPC has been contacted to ensure that all obligations under the Act are fulfilled and, provide information about how to submit a complaint to the IPC.

The employee involved in the breach shall document the incident in detail in writing, including how each step in the above process was executed.

11. APPENDICES

Appendix A – MFIPPA Process Map

Appendix B – Records Retrieval Form



Text	Prepared by	Date
Process	Approved by	Date
MFIPPA REQUEST PROCESS		

Appendix B – RECORDS RETRIEVAL FORM

MFIPPA RECORDS RETRIEVAL FORM

To be completed and returned to the Manager of Records and Information Services

1. Indicate the places that were searched (e.g., what files in which offices or file rooms, which shared drives or software applications):	
2. Indicate methods/processes used to conduct the search and types of files searched (e.g., searching electronic files, paper files, file lists, off-site file lists, microfiche etc.):	
3. Length of time required to do the search:	
4. Responsive records located? (Indicate if responsive records no longer exist but did exist at one time (i.e., provide the number of the Records Retention Schedule which authorized the destruction of those records):	Yes No
5. Are there any concerns with these records or this request? (If yes, please explain):	Yes No
6. Would you like to be provided with a copy of the responsive records?	Yes No
7. Would you like to be advised when responsive records are released?	Yes No

Name:	
Date(s) of search:	