MUNICIPALITY OF Thames Centre

Policy: Access to Records and Protection of Personal Privacy Policy

Policy Number: CP-A-9.4

Effective Date:

Approval: *date approved by CAO*

Disclaimer: If required, interpretation is subject to the discretion and authorization of the Chief Administrative Officer. All policies are subject to change without notice.

POLICY STATEMENT:

This “Access to Records and Protection of Personal Privacy” Policy is a general guide to the *Municipal Freedom of Information and Protection of Privacy Act* (“MFIPPA” or “Act”).

This policy applies to all employees, volunteers and Members of Council of the Municipality of Thames Centre. It governs the procedure on how the Municipality responds to access requests and how it protects personal information, as required under MFIPPA.

The policy combines current practices 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.

DEFINITIONS:

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

“CAO” means the Chief Administrative Officer of the Municipality of Thames Centre or written designate.

“Clerk” means the Clerk of the Municipality of Thames Centre or written designate.

“**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*.

“**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.

“Privacy Breach” means a breach that occurs when personal information is collected, retained, used, accessed or disclosed in ways that are not in accordance with the provisions of the Act.

“**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.

“Privacy Impact Assessment” and **“PIA”** (IPC Guide), is a risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology, program, process or other activity may have on an individual’s privacy.

“Project” (IPC Guide) in relation to a PIA, means any work involving the collection, use, retention, disclosure, security and disposal of personal information. This may include a new program, process, service delivery model or an information technology system or changes to an existing program, process or system.

“Relevant Department” means the primary municipal department to which the records request pertains to.

“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.

PRINCIPLES:

The following principles will form the basis of this policy:

Transparency

The Municipality of Thames Centre is committed to:

- Promoting an open and transparent government
- The Routine Disclosure and the Active Dissemination of records, when consistent with the principles and rules of the Act
- Providing access to records and information, in accordance with the principles and rules of the Act.

Accountability

The Municipality of Thames Centre shall:

- Take reasonable steps to protect the collection, use, access and disclosure of personal information.
- Facilitate an individual’s right of access as well as the ability to correct their personal information in the custody or under the control of the Municipality, subject to any legislative exemptions.

ROLES & RESPONSIBILITIES:

The “Head”:

According to By-law 10-2011, the Council has designated the Clerk as Head to the Clerk under the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), in accordance with Section 3 of the Act. This delegation is further confirmed by Delegation By-law No. 51-2024, which was passed by Council on June 24, 2024.

The Head is accountable for decisions under the Act and for overseeing how the Municipality generally administers the Act. 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.

For the purposes of this policy, the Head is responsible for:

- Exercising the duties pursuant to Council's delegation 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 while communicating with the CAO;
- 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 Directors and the Chief Administrative Officer to resolve any delays by municipal 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;
- Reporting and investigating privacy breaches;
- Providing training to employees on the Act;
- Administering, monitoring, and promoting all aspects of this policy.

People Leaders:

Those who have employees reporting directly to them are responsible for:

- Ensuring that the employees they oversee adhere to the procedures in this policy and the provisions of the Act;
- Allocating sufficient employees and other resources to ensure that municipal departments 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 departmental records in compliance with Thames Centre's current Records Management Policy;
- Assisting the Head with a completed Records Retrieval Form (**Appendix "B"**);
- Follow the guidelines for transmitting personal information, as outlined in this Policy;
- Being mindful of different potential privacy breaches and prevent whenever possible (example: locking your computer if away, avoid leaving laptop in the car);
- Use personal information only for its intended purpose of collection
- If a privacy breach is suspected, reach out to the Head immediately
- Reach out to the Head to ask questions if needed

Municipal Employees and Volunteers:

All employees of the Municipality of Thames Centre shall be aware of and comply with this policy as required and shall also be responsible for:

- Maintaining departmental records in compliance with Thames Centre’s current Records Management Policy;
- Locating, retrieving and providing copies of records to the Head by the deadlines provided, in response to a request made under the Act;
- Participating in MFIPPA and Records Management training;
- Providing additional information to the Head with respect to requests made under the Act (example: search time estimates, clarification requirements, concerns with records, etc.);
- Assisting the Head with a completed Records Retrieval Form (**Appendix “B”**);
- Follow the guidelines for transmitting personal information, as outlined in this Policy
- Being mindful of different potential privacy breaches and prevent whenever possible (example: locking your computer if away, avoid leaving laptop in the car);
- Use personal information only for its intended purpose of collection
- If a privacy breach is suspected, reach out to the Head or designate immediately
- Reach out to the Head or designate to ask questions if needed

Failure to comply with this Policy may result in disciplinary action up to and including termination.

This Policy will be reviewed on an annual or as needed basis.

ACCESS REQUEST PROCEDURES:

Timely Response to Access Requests

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

An extension may be requested, however, if the Head does not respond to a request within the 30-day time period, the request is then deemed to have been refused. The Act then entitles requesters to appeal immediately the “deemed refusal” to the IPC.

Because of the legislated timeframes, employees should process FOI requests on a priority basis. The Head will notify the applicable Director or department head in writing, requesting records with a specific deadline for the responsive records to be provided. Generally, 10 business days are allocated for staff to complete the search and provide copies of responsive records to the Head.

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

Follow-up Process

If the department 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 in the following consecutive steps:

- Provide up to two (2) reminders directly to the department
- If still no response, send communication to the Director *(if applicable)*
- If still no response, send communication to the Chief Administrative Officer

Receiving Requests

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

The Head will seek to determine whether a requester may obtain access to all or some of the requested records directly from the relevant municipal department – for example, by providing information that is public.

Municipal departments should follow the current "Routine Disclosure and Active Dissemination" policy whenever possible, outside of the formal Freedom of Information (FOI) records access procedure. If the relevant department has any questions, they shall inquire with the Head.

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")

Once the Head has clarified the request, the Head shall notify the Director of the relevant department in writing (as well as the department head and/or any other staff members). The notification shall include the exact wording of the requested records, the Records Retrieval Form (see **Appendix "B"**), and the due date for submission.

The relevant department 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 written notification. 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.

Staff members from the relevant department may identify other departments that may also have responsive records.

Under extraordinary circumstances, requests that require searches of the Microsoft Exchange System can be forwarded directly to the Middlesex County Information Technology (IT) Department, with the approval of the Chief Administrative Officer.

The relevant department is required to notify the Head within three (3) days of receipt of the written notification, if it is anticipated that a search for responsive records will take more than one (1) hour. If the search is anticipated to take an hour or less, the relevant department shall provide copies of records (electronically or photocopies) by the deadline provided in the written notification.

If a time extension is required to complete a search, the relevant department should contact the Head immediately to determine whether the Act permits a time extension. The relevant department is required to justify search time estimates and requests for time extensions in writing, if applicable.

The Records Retrieval Form (see **Appendix "B"**) may be completed and returned with the responsive records, which indicates actual time spent searching for the records, the location and methods used to search for records, and/or whether there are any concerns with the records in question. This form may be submitted even if no records are provided in response to the request.

In the event of an appeal, the IPC may call on the Head to describe the steps taken to conduct the search. Referencing the Records Retrieval Form in such instances assists the Head during the appeal process.

At the request of the Director or staff of the relevant department, the Head will advise when the records pertaining to their department will be released. The Head will also upon request provide copies of the records to be released prior to their release, where legislative timelines allow. The Head must provide copies of the records to be released prior to their release to the Communications Manager.

Time Extensions

The Head determines extensions for a request based on input from the relevant department. 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 requires searching through a large number of records and meeting the time limit would unreasonably interfere with day-to-day municipal operations; or

2. Staff must consult with an external agent to comply with the request and cannot reasonably complete the consultation within the time limit.

If either of the above factors apply, the reasons for an extension shall be summarized in writing by the Head as follows:

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

   - explain the steps required for employees to search for responsive records and estimating the total number of pages of records;
   - identify any exemptions that may be applicable to the records; and
   - provide 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 to be consulted;
   - why consultation is necessary; and,

- an estimate of when the consultation will be complete.

Requirements of Records Provided

The relevant department shall provide all of the responsive records to the Head by the deadline provided, using the following guidelines:

- Whenever possible, records shall be emailed directly to the Head (or designate).
- For larger numbers of records – records may be temporarily saved in the Network Drive, in OneDrive, or on a USB flash drive. Once the Head has confirmed receipt of the records, the records shall be deleted from the transitory location.
- Records (electronic or paper) must be provided unaltered. Records will not be accepted that have been redacted or "blacked-out".
- Original paper records are to be copied or scanned and emailed to the Head. Copies must be legible.
- A completed Records Retrieval Form (**Appendix "B"**) must be submitted with the records by the deadline.
  - If the relevant department has any identified areas of concern in any of the responsive records, this must be recorded in writing on the Records Retrieval Form, noting that the Head has the final decision.

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 Municipality of Thames Centre who has the authority to make decisions on disclosure under the Act.

The Head will consider any concerns from the relevant department, as recorded on the Records Retrieval Form, noting that the Head has the final decision.

The Head may refuse access to a record and may sever part of a record for reasons including but not limited to:

- the information is subject to a legal privilege;
- another act or a court order prohibits its disclosure to the individual;
- the request is frivolous or vexatious or made in bad faith;
- advice or recommendations of a public servant, any other person employed in the service of an institution or a consultant retained by an institution;
- where the disclosure would interfere with a law enforcement matter;
- reveals information received in confidence from another government or its agencies by an institution;
- reveals a trade secret or scientific, technical, commercial, financial or labour relations information, supplied in confidence implicitly or explicitly;
- Further exceptions as outlined in the Freedom of Information and Protection of Privacy Act such as: Third party information, Economic and other interests of Ontario, Information with respect to closed meetings, Solicitor-client privilege, Danger to safety or health, Personal privacy, Species at risk, Information soon to be published, etc.

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.

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 Municipality 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.

The Head further has discretion about how to inform the requester when one of the following access exceptions apply. The Head can choose to specifically indicate the exception that applies — or to indicate that one of them applies, without specifying which one. The Head can also refuse to confirm or deny the existence of any record subject to these exceptions:

- the information was collected or created primarily in anticipation of or for use in a legal proceeding which has not concluded, or
- granting access could reasonably be expected to:
  - result in a risk of serious harm to any individual
  - lead to the identification of an individual who was required by law to provide information in the record to the service provider or
  - lead to the identification of an individual who provided the information either explicitly or implicitly in confidence, if you consider it appropriate to keep their identity confidential

Fees

For all requests under MFIPPA, the requester must pay a $5.00 application fee. The application fee is mandatory and cannot be waived.

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 Municipality 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 Municipality

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

The Head shall, before giving access to a record, give the person requesting access a reasonable estimate of any amount that will be required to be paid under this Act that is over $25.

Councillors' Records

The Head, in consultation with the CAO, will assist in determining whether a record of a Member of Council is a corporate record and consider the specifics of each request in light of a number of **principles established by the IPC**.

Councillors' records may be 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.

Appeals to the Information and Privacy Commissioner (IPC)

The Act establishes the right of a requester to appeal decisions that the Head makes regarding 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 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").

In the event that the Commissioner issues an order with respect to access to records, the Head will notify the appropriate Director of the relevant department. The Head will ensure compliance of the issued order.

Should the IPC notify the Head that the Commissioner will be entering and inspecting any premise occupied by the Municipality of Thames Centre for the purposes of an investigation, the Head will notify the Chief Administrative Officer and the Director of the relevant department. The Head shall 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.

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 Municipality, employees or consultants acting on the Municipality'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 for the proper administration of a lawfully authorized activity.

The Municipality 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;

- where the IPC has authorized the Municipality 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 Municipality must provide the individual with a **Notice of Collection** statement that contains:

- the Municipality'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.

Staff shall only use personal information for the specific purpose for which it was collected.

Personal information does not include information about an individual who has been dead for more than thirty years. Personal information also does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity. This applies even if an individual carries out business, professional or official responsibilities from their dwelling and the contact information for the individual relates to that dwelling. Specific to the *collection* of personal information, the definition of personal information includes information that is not recorded.

Retention of Personal Information

Personal information that has been collected by the Municipality must be retained for at least one year after it is used, unless another retention period has been provided in the Municipality'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 Municipality shall take reasonable steps to ensure that personal information is not used unless it is accurate and up to date. The Municipality must create a record of any use of personal information that is different from how the information is used on a regular basis.

The Municipality is only permitted to use personal information when the individual has consented to the particular information being used for:

- the purpose for which it was obtained or compiled;
- a consistent purpose, (example: the individual might reasonably expect the use); or
- the purpose for which the information was disclosed to the Municipality under FIPPA.

Disclosure of Personal Information

The Municipality is only permitted to disclose personal information in the following circumstances, in compliance with the Act;

- if the individual has consented to its disclosure;
- for the purpose for which it was obtained;
- for a consistent purpose, (example: 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.

Transmitting Personal Information

When employees are required to transmit personal information to parties external to the organization, the following guidelines should be considered to help ensure that personal information is protected from unauthorized access or disclosure:

- Where possible, hand deliver the information.
- Where possible, apply a password to the document.
    - Send the password to the external party in a separate message or over the phone.
- If using OneDrive, configure the security settings to ensure only specific email addresses may open the link to the folder.
- Ensure confirmation of the transfer with the external party. Once confirmed received, delete the OneDrive link and/or email message.
- If necessary to send through the mail, consider using Registered Mail or a Courier Service to deliver hard copies of the personal information and request a signature upon receipt.
- Where possible, avoid sending personal information via facsimile (fax).

Offence

Any person who willfully 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 Municipality of Thames Centre has improperly collected, used, disclosed, retained or disposed of their personal information.

If an individual submits a complaint and an investigation is initiated, the Head shall receive notice from the IPC. The Head shall, in consultation with appropriate staff, represent the Municipality during a privacy complaint investigation. The responsible employee(s) will cooperate and assist the Head during the course of the investigation.

Responding to a Privacy Breaches Under the Act

Please refer to the current “Privacy Breach” Policy for protocol on responding to a privacy breach under the Act.

Privacy Impact Assessment (PIA)

A PIA is used to assess compliance with MFIPPA; it aims to identify and address the privacy impacts of proposed projects or activities.

Before staff implement a project or activity that involves the collection of personal information, they shall consult with the Head, who will determine whether a PIA is required. Staff may be required to conduct a preliminary assessment to assist the Head in making this determination.

A PIA may be required where the Head determines the collection is at a large scale; where the personal information is deemed sensitive; or where the collection, use, or disclosure of the personal information impacts decision-making.

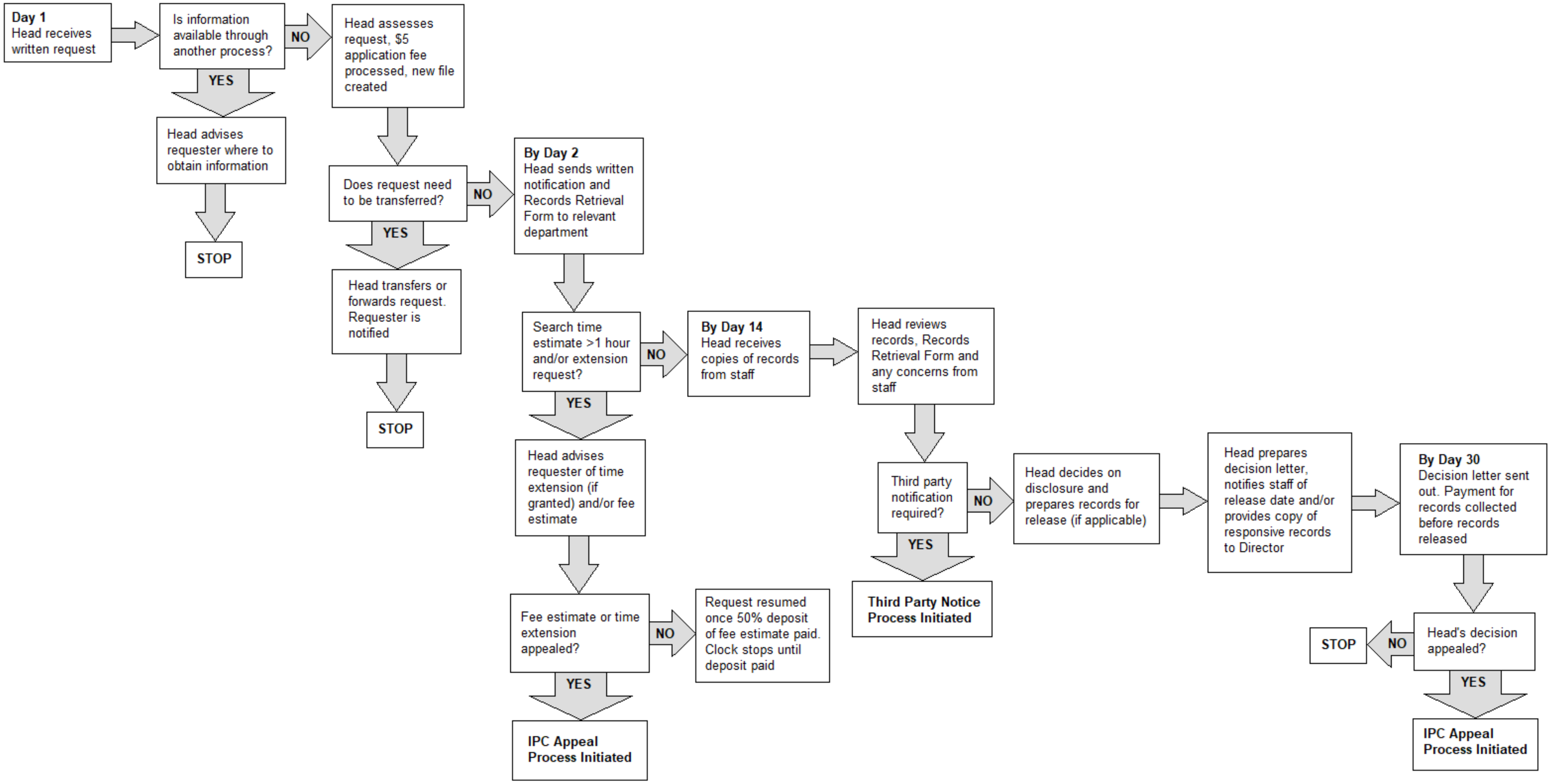
When the Head determines a PIA is required, staff shall conduct a PIA, in consultation with the Head, prior to the implementation of the project or activity. Staff will be supplied with a PIA template to conduct the assessment.

Once the PIA is completed by staff, it shall be reviewed and/or approved by the Head. If recommendations are made by the Head to implement controls related to the protection of personal information or compliance with legislation, those recommendations shall be adopted by staff prior to initiating the activity or program.

Accessibility

Records that are disclosed are subject to the requirements of the Municipality’s Accessibility Policy and *the Accessibility for Ontarians with Disabilities Act* and will be provided in accessible formats upon request.

Appendix “A” – MFIPPA Freedom of Information (FOI) Requests – Process Map


Day 1 Head receives written request
Is information available through another process?
NO
Head assesses request, $5 application fee processed, new file created
YES
Head advises requester where to obtain information
STOP
Does request need to be transferred?
NO
By Day 2 Head sends written notification and Records Retrieval Form to relevant department
YES
Head transfers or forwards request. Requester is notified
STOP
Search time estimate >1 hour and/or extension request?
NO
By Day 14 Head receives copies of records from staff
Head reviews records, Records Retrieval Form and any concerns from staff
YES
Head advises requester of time extension (if granted) and/or fee estimate
Third party notification required?
NO
Head decides on disclosure and prepares records for release (if applicable)
Head prepares decision letter, notifies staff of release date and/or provides copy of responsive records to Director
By Day 30 Decision letter sent out. Payment for records collected before records released
YES
Third Party Notice Process Initiated
Fee estimate or time extension appealed?
NO
Request resumed once 50% deposit of fee estimate paid. Clock stops until deposit paid
YES
IPC Appeal Process Initiated
Head's decision appealed?
NO
STOP
YES
IPC Appeal Process Initiated

Appendix "B" – Records Retrieval Form

To be completed and returned to the Head of MFIPPA

Name: ________________ Department: _________________ Date: ______________

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 (example: searching electronic files, paper files, etc.):

____
____
____

3. Length of time required to complete search: ________________________________

4. Responsive records located? (Indicate if responsive records no longer exist but did exist at one time (example: provide the authorization of 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**