Policy: Privacy Breach Policy

Policy Number: CP-A-9.5

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:

The Municipality of Thames Centre is committed to protecting personal information in the custody or control of the Municipality and complying with the privacy protection requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act ("MFIPPA" or "the Act").*

BACKGROUND:

The *Municipal Freedom of Information and Protection of Privacy Act* provides the right of access to information under the control of institutions in accordance with the principles and protects the privacy of individuals with respect to personal information about themselves held by institutions, and to provide individuals with a right of access to information.

Sections 31 & 32 of the *Municipal Freedom of Information and Protection of Privacy Act* outlines when an institution can use and/or disclose personal information in its custody or under its control. When the use or disclosure of personal information or records containing personal information violates Sections 31 or 32 of the Act or any other applicable legislation, a privacy breach occurs. Privacy breaches can also occur when personal information of residents or employees is stolen, lost or mistakenly disclosed (example: personal information is mistakenly mailed/emailed to the wrong person).

PURPOSE:

The purpose of this policy is to ensure that all Municipality of Thames Centre employees, volunteers and Members of Council comply with the privacy protection requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act.*
This policy confirms the Municipality's obligation to protect personal information in its custody and control. Privacy breaches undermine public trust in the Municipality and may result in significant harm to the Municipality and to those whose personal information is

collected, used or disclosed inappropriately.

This policy outlines the steps that shall be followed when an alleged Privacy Breach is reported, to ensure that quick containment is accomplished, and an investigation initiated to mitigate the potential for further dissemination of personal information.

The CAO in conjunction with the Clerk is responsible for the overall implementation and enforcement of this Policy and can delegate duties within this policy as deemed appropriate.

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

This Policy will be reviewed on an annual basis or as needed by the Clerk and CAO.

DEFINITIONS:

"Act" means the *Municipal Freedom of Information and Protection to Privacy Act, R.S.O. 1990, Chapter M. 56*.

"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.

"Employee" means any paid employee, including, but not limited to, full-time, part-time, paid apprenticeships, and seasonal employees.

"Investigator" means a person appointed by the CAO, which could be an employee or a third party, to conduct an investigation into a privacy breach.

"Municipality" means the Corporation of the Municipality of Thames Centre.

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

a) Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or martial 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" 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 copy thereof; and

b) Subject to regulations, any record that is capable of being produced from a machine readable record under the control of an institution by means of a computer hardware and software of any other information storage equipment and technical expertise normally used by the institution.

GENERAL PROCEDURE:

A privacy breach occurs when personal information is collected, retained, used, accessed 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.

The following examples would demonstrate a privacy breach:

- An institution or employee intentionally or unintentionally discloses records containing personal information
- A system is broken into by an unauthorized user (hacker)
- Personal information may be lost (a file misplaced within an institution)
- Stolen equipment (laptop, corporate cell phone)
- Inadvertently disclosed through human error, such as misplaced personal information placed in a blue box, instead of being shredded
- A letter addressed to person A is actually mailed to person B

Privacy breaches undermine public trust in the Municipality and may result in significant harm to the Municipality and to those whose personal information is collected, used or disclosed inappropriately. It also may result in legal action taken against the Municipality, employee or third-party consultant or contractor.

The following protocol shall be adopted during a breach or a potential breach of personal privacy, as per **IPC Guidelines**.

The Municipality's highest priority is to quickly respond to a privacy breach with preventative measures to avoid future privacy breaches. When a privacy breach is alleged to have occurred, municipal staff shall undertake immediate action. In all instances of a privacy breach (or alleged breach), the following procedure, conducted in quick succession, or concurrently, shall be followed:

Step 1: Confirm

The purpose of the confirmation is to begin to assign responsibilities so that the rest of the breach may be followed in a timely and complete manner. If a complaint has been received or an employee suspects a privacy breach has occurred, contact the CAO and Clerk immediately. The CAO will designate an investigator to handle the breach, depending on the type of breach, who will then investigate the validity of the complaint or suspicion.

The "Risk Assessment Chart" attached hereto as Appendix A, will be used to assist in determining if a privacy breach occurred. If a privacy breach is confirmed, the CAO or investigator will evaluate the severity of the breach and proceed accordingly.

Upon confirmation that a privacy breach has occurred, the following steps should be taken:

1. Document the particulars of the incident
2. Determine if and what personal information was disclosed
3. Report the breach to CAO and Clerk

The CAO shall handle all inquiries with respect to privacy breaches and the actions of the Municipality, in response to an alleged or confirmed breach.

Step 2: Contain

The CAO or investigator shall, in cooperation with other staff, undertake the following actions to contain the privacy breach:

4. Retrieve and secure any records associated with the alleged breach. If the recipient of personal information states they have destroyed the information, written confirmation is required.

5. Determine if the breach would allow unauthorized access to other potential additional personal information (example: electronic information system)

6. Isolate and suspend the process(es) that caused the privacy breach. This may include:

    a) Changing passwords/codes
    b) Shutting down computer applications affected

c) Suspending mailings
d) Replacing locks on doors, filing cabinets etc.

7. Secure any evidence or documentation relating to the specific circumstances of the breach.

8. Document the breach and all containment activities.

9. Meet with staff to provide instructions and updates on the breach.

10. In case of theft of equipment, break in or any criminal activity:

a) Contact the Police and file a report
b) Communicate the issue to staff and Council
c) Contact Municipal Legal Support

Step 3: Investigate

The CAO or investigator shall conduct an internal investigation as to what caused the privacy breach, once the breach has been contained. This includes reviewing all policies and procedures and/or staff actions that caused the breach, which helps in developing mitigation procedures for future breaches. Breaches that are reported to the Information Privacy Commission will require detailed submissions including all information above.

The investigation shall:

11. Identify and analyze the events that lead to the breach, including interviewing staff and collection of statements
12. Evaluate containment measures
13. Recommend remedial action so future breaches do not occur, review staff training and responsibilities involved in the breach.

Step 4: Notify

As required, the CAO or investigator shall notify all individuals whose personal information was compromised, through a letter substantially in the form of attached Appendix B. The purpose of providing notice of the privacy breach to affected individuals is to provide the following information:

- What happened to cause the breach;
- The specific personal information affected;
- The nature of the potential or actual risks;
- Steps, if any, taken so far to control or reduce the harm;
- What actions are being taken to prevent future privacy breaches;
- How the individual can protect themselves; and
- Contact information for municipal staff

This notice will also contain the required information about an individual's right to

complain to the Information and Privacy Commission (IPC) about the handling of their private information, as well as the contact information for the IPC.

The Clerk shall notify the IPC of the breach if:

- The personal information is highly sensitive;
- There is a large number of affected individuals;
- There is difficulty in containing the breach; or
- The breach poses a real risk of significant harm.

If the Information and Privacy Commission needs to be notified, all mitigation strategies will need to be detailed in the official submission, along with all notifications provided to affected parties. The Clerk, as head of Municipal Freedom of Information and Protection of Privacy, will be the point person for the Information and Privacy Commission (IPC).

The CAO or investigator shall determine if other authorities or organizations, such as law enforcement, the privacy commissioner's office and/or professional or regulatory bodies should be informed of the breach.

Step 5: Mitigate

Following the completion of an investigation, the CAO or investigator shall prepare a report outlining the results of the investigation, including any recommendations to mitigate future incidents. Any recommendations from the report will be reviewed and where appropriate, implemented. A copy of the report shall be made available to all parties who were affected by the breach and if necessary, submitted to the IPC.

A report to Council shall be done if the breach included:

1) More than five (5) individuals are affected by a confirmed breach; or
2) In the opinion of the CAO or investigator it is determined that it is in public interest to provide such a report.

If required, the CAO or investigator may also:

- Examine the relevant information management systems to enhance compliance with privacy legislation;
- Develop and implement new security or privacy measures
- Review, amend or reinforce any existing policies, procedures and/or practices
- Develop new policies, procedures and/or practices
- Conduct Privacy Impact Assessments (PIA) before introducing or changing technologies, information systems and processes to ensure privacy risks are identified and addressed
- Provide staff training where needed

- Seek input from appropriate parties such as Middlesex County legal, the Ontario ministry responsible for information and privacy matters, or the IPC.

Forms

1. Appendix A – Privacy Breach Risk Assessment Chart
2. Appendix B – Privacy Breach Letter Template
3. Appendix C – Reporting a Privacy Breach Note(s)

Appendix A

Municipality of Thames Centre Privacy Breach Risk Assessment Chart

The "Risk Assessment Chart" can be used to assist in determining if a privacy breach occurred. If you answer "No" to all risk factors, there is a low probability that personal information has been compromised and it's not likely a reportable breach. Regardless, the CAO or investgator will make the determination.

	Risk Assessment	Yes or No
1.	**Risk of identity theft** Is there a risk of identity theft or other fraud? Identity theft is a concern if the breach includes unencrypted information such as names in conjunction with social insurance numbers, credit card numbers, driver's licence numbers, personal health numbers, debit card numbers with password information or any other information that can be used for fraud by third parties (e.g. financial information)	
2.	**Risk of physical harm** Does the loss of information place any individual at risk of physical harm, stalking or harassment?	
3.	**Risk of hurt, humiliation, damage to reputation** Could the loss of information lead to hurt, humiliation or damage to an individual's reputation? This type of harm can occur with the loss of information such as medical or disciplinary records.	
4.	**Risk of loss of business or employment opportunities** Could the loss of information result in damage to the reputation to an individual, affecting business or employment opportunities?	

Appendix B

DATE

NAME

Dear **XXXX**,

NOTIFICATION OF PRIVACY BREACH

I am writing to inform you that a breach of privacy occurred at the Municipality of Thames Centre office which involved your personal information. A privacy breach may be defined as an incident involving unauthorized disclosure of personal information in the custody or control of an institution covered by Ontario's *Municipal Freedom of Information and Protection of Privacy Act*.

Information about the Breach

The Municipality of Thames Centre was able to retrieve all of the records, including yours, from **[Company Name]** shortly after we were made aware of the privacy breach. The owner of **[Company Name]** has assured us in writing that no copies of these records have been retained. In addition, the Municipality has taken action to change our procedures at **(office)** to ensure this type of privacy breach will not happen again and we are initiating privacy awareness training for our **(office)** supervisors.

The Municipality of Thames Centre has **(or has not)** contacted the Ontario Information and Privacy Commission about this incident. You have the right to make a complaint to the Information and Privacy Commission and if you choose to do so, you may contact them at 2 Bloor Street East, Suite 1400, Toronto, On M4W 1A8.

Clerk
Municipality of Thames Centre

Appendix C

Reporting a Privacy Breach
Notes

Date: _____

Staff Name: _____

Person Reporting Breach:

Name: _____

Address: _____

Telephone Number: _____

Email Address:_____

Reported Breach:

Measures taken to retrieve information:

Date/Time Reported to CAO & Clerk: _____