Municipality of West Elgin

Schedule "A" to By-Law #2020-92

Policy AD-8.1
Privacy Breach Policy

Effective Date: December 17, 2020

Review Date:

1. Policy Statement

The Municipality of West Elgin is committed to protecting the personal information in the custody or control of the municipality and comply with the privacy protection requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act.*

2. 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 to protect 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 *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 *Municipal Freedom of Information and Protection of Privacy 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).

3. Purpose

The purpose of this policy is to ensure that all Municipality of West Elgin employees 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.

4. Scope and Responsibility

This policy applies to all employees, volunteers, agents, contractors and Members of Council for the Municipality of West Elgin.

The Chief Administrative Officer (CAO) and Clerk are responsible for the overall implementation and enforcement of this policy, as directed by the *Municipal Freedom of Information and Protection of Privacy Act.*

5. Definitions

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

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

"Municipality" means the Corporation of the Municipality of West Elgin.

"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 medial, 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 the use or disclosure of Personal information or records containing personal information in violation of Section 31 or 32 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.

6. General Procedure

Privacy Breach is an activity that resulted in the event of an inappropriate use of Personal Information (PI) or disclosed the Personal Information to the wrong recipient. A privacy breach may result in legal action taken against the municipality, employee or third-party consultant/contractor. Examples can include the loss or theft of a laptop, mailing sensitive information to the wrong address or disclosing personal information over the phone without appropriate consent of the individual. The Municipality's highest priority is to respond to a privacy breach with immediate possible preventative measures to avoid future privacy breaches.
The following examples would demonstrate the privacy breach:

- An institution or employee intentionally or unintentionally discloses records containing personal information
- A municipal facility is broken into an personal information is stolen (laptop)
- 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 a placed personal information in blue box, not shredded
- A letter addressed to person A is actually mailed to person B

6.1. 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 if an employee suspects a privacy breach has occurred the CAO & Clerk will 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 & Clerk will evaluate the severity of the breach and proceed accordingly.

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

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

6.2. Step 2: Contain

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

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

2. Determine in the breach would allow unauthorized access to any other personal information (example: electronic information system)

3. Isolate and suspend the process 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.

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

5. Document the breach and all containment activities.

6. Meet with staff to provide instructions and update them on what is happening.

7. In case of theft of equipment or 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

6.3. Step 3: Investigate

The CAO & Clerk shall conduct an internal investigation as to what caused the privacy breach, once the breach has been contained. Including all policies and procedures and/or staff actions that caused the breach. This is done to develop 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:

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

6.4. Step 4: Notify

The Clerk shall notify, as required, the individuals whose personal information was compromised, through a letter substantially in the form of attached Appendix B. The purpose of providing notice of privacy breach to the individuals whose personal information was involved in the incident is to provide them with information about what happened, the nature of the potential or actual risks, what mitigating actions are being taken and the appropriate action for the individual to take to protect themselves. Along with the required information about an individual's right to complain to the Information and Privacy Commission about the handling of their private information and the contact information for the IPC.

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

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

6.5. Step 5: Mitigate

Upon completion of the investigation and documentation the CAO & Clerk shall:

1. Review the relevant information management systems to enhance compliance with privacy legislation
2. Amend or reinforce the existing policies, procedures and practices for managing and safeguarding personal information

3. Develop and implement new security or privacy measures, if required
4. Review policies and staff training

A report shall be prepared by the CAO & Clerk outlining the results of the investigation, including any recommendations to mitigate future breaches. Any recommendations from the report will be reviewed and where appropriate implemented. Consistent with best practices 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 & Clerk it is determined that it is in public interest to provide such a report.

7. 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 West Elgin 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 & Clerk 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 West Elgin 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 West Elgin 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 West Elgin 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.

Jana Nethercott,
Clerk
Municipality of West Elgin

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: _____