Protocol Name: Privacy Breach Protocol
Policy Number: A17-Administration- 001-2019
Section: Information and Access and Privacy
Effective Date: January 1, 2019
Supersedes: n/a
Last Revision: n/a
Schedule for Review: January 1, 2021

1. **Purpose**

All Municipality of South Huron employees and Council Committee members shall, at all times, comply with the privacy protection requirements as mandated by the *Municipal Freedom of Information and Protection of Privacy Act.*

This protocol affirms the Municipality of South Huron's obligation to protect personal information in the custody or control of the institution. Privacy Breaches undermine public trust in an institution and may result in significant harm to the municipality and to those whose personal information is collected, used or disclosed inappropriately.

This protocol requires the immediate reporting of all Privacy Breaches and alleged Privacy Breaches to the Clerk and outlines the steps to be followed when an alleged Privacy Breach is reported. This process will ensure that when an alleged Privacy Breach is discovered, it is quickly contained and investigated to mitigate the potential for further dissemination of personal information. Furthermore, the investigation shall recommend remedial steps focused on preventing similar events in the future.

2. **Sources**

Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter 56

Privacy Breach Protocol: Guidelines for Government Organizations, Information and Privacy Commissioner of Ontario

3. **Scope**

This protocol applies to all Municipality of South Huron employees, volunteers, agents, contractors and members of Council.

4. **Definitions**

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

"IPC" – means the Information and Privacy Commissioner of Ontario

"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, 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 view 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 Sections 31 or 32 of the Act. Breaches can be intentional or accidental.

"Record" – means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, and includes any Record as defined by Section 2(1) of the Act.

5. Procedure

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) set out rules that persons or organizations must follow when collecting, using, disclosing, retaining, and disposing of personal information.

Protocol Name: Privacy Breach Protocol
Policy Number: A17-Administration- 001-2019
Section: Information and Access and Privacy
Effective Date: January 1, 2019
Supersedes: n/a
Last Revision: n/a
Schedule for Review: January 1, 2021

The Act balances the rights of individuals to their privacy with the legitimate needs of organizations to collect, use and share information to conduct their work. The Act also requires organizations to take reasonable steps to ensure that information in their custody or control is protected against theft, loss, unauthorized use, disclosure, modification, or disposal.

When a person becomes aware of a privacy breach, timely assistance and remedial steps are vital to minimizing harm, while demonstrating accountability and restoring trust.

When a Privacy Breach is alleged to have occurred municipal staff will undertake immediate action. In all instances of a Privacy Breach or alleged breach the following steps, conducted in succession or concurrently will be followed:

Step 1: Identify and Alert

Identify the suspected source of the alleged Privacy Breach (ie. record systems or websites) that are believed to have been the source of the potential Privacy Breach and alert a supervisor or manager within the area of the alleged Privacy Breach. The supervisor or manager will notify the Clerk immediately. If a supervisor or manager is unavailable, staff will contact the Clerk and advise of the alleged Privacy Breach.

Upon notification, the Clerk will establish a response team with representatives from the following areas to manage South Huron's response to the alleged breach:

- Clerk's Department
- Department where the alleged breach occurred
- Other areas where appropriate

A meeting involving the members of the response team shall occur as soon as practicable after notice is provided to the Clerk of the alleged Privacy Breach. During this meeting, the response team will attempt to establish the particulars of the incident, including:

- the location and date of the incident and discovery
- the cause of the incident, if known

- an estimate of the number of individuals involved
- the type of individuals involved (e.g. internal vs. external)
- the type of Personal Information subject to the breach
- any identifiable Records associated with the alleged breach
- any actions already undertaken to contain the breach
- other organizations who have been notified (e.g. police)

This information will be used to develop a containment strategy and notify the affected individuals.

After the initial meeting, the Clerk will advise the Chief Administrative Officer of the known circumstances and provide updates as appropriate throughout the process.

Step 2: Contain

The Clerk will require the co-operation of the manager and staff as appropriate and undertake the following actions to contain the alleged Privacy Breach:

- retrieve and secure any records associated with the alleged breach;
- where appropriate and depending on circumstances, isolate and suspend access to any system associated with the alleged breach;
- suspend all processes or practices that are believed to have served as a source for the alleged breach;
- take any other action necessary to contain the alleged breach.

Step 3: Notify

The Clerk may at his or her discretion notify the IPC of all confirmed Privacy Breaches.

The Clerk's Office will be responsible for notifying all individuals affected by a Privacy Breach by either telephone or in writing. This notification will include information surrounding the nature of the alleged, or confirmed Privacy Breach, the details of the breach as understood at the time of notification, the specific personal information affected and contact information for the Clerk and the Information Privacy Commissioner of Ontario, should there be additional questions.

Protocol Name: Privacy Breach Protocol
Policy Number: A17-Administration- 001-2019
Section: Information and Access and Privacy
Effective Date: January 1, 2019
Supersedes: n/a
Last Revision: n/a
Schedule for Review: January 1, 2021

The Clerk's Office will handle all inquiries with respect to Privacy Breaches and the actions of the institution in response to an alleged or confirmed breach.

Step 4: Investigate

After using best efforts to contain the alleged Privacy Breach and notifying the affected individuals, the Clerk shall undertake an investigation in an attempt to establish:

- whether a Privacy Breach occurred;
- a chronology of events;
- the sources of the breach, including policies or procedures responsible;
- the nature and sensitivity of the Personal Information disclosed;
- the number of individuals affected;
- the individuals or category of individuals who were affected; and
- any other factors relevant to the circumstances.

The investigation will review existing policies and procedures governing the protection of Personal Information and make recommendations intended to strengthen the protection of such information collected and used in the area.

Step 5: Report and Follow-Up

After completing the investigation, a report shall be prepared by the Clerk outlining the results of the investigation, including any recommendations to mitigate future incidents. Consistent with privacy best practices, a copy of the report shall be forwarded to the IPC, as well as, to all individuals who were affected by the breach.

In the matter of transparency and accountability, this report should also be included on a future Council agenda where:

- more than five (5) individuals are affected by a confirmed breach; or
- in the opinion of the City Clerk, in consultation with the Chief Administrative Officer, it is determined that it is in the public interest to provide such a report.

Recommendations from the report will be included in updated municipal policies.