Town of Whitby Procedure

Procedure Title:	Privacy Breach Protocol
Procedure Number:	CA 060-002
Reference:	Corporate Access and Privacy Policy (CA 060)
Date Approved:	July 26, 2016
Date Revised:	June 2, 2023
Approval:	Chief Administrative Officer
Point of Contact:	Manager, Information & Content Services, ext. 2855

Purpose

The purpose of this Procedure is to outline the Response Protocol to follow when a suspected Privacy Breach may have occurred.

Scope

This Procedure applies to all Town staff, volunteers, agents, contractors, and Members of Council.

Note: When a suspected Privacy Breach may have occurred, Town staff shall undertake immediate action. In all instances of a Privacy Breach, the Response Protocol shall be conducted in quick succession, or concurrently.

Index

1. Definitions

1.1. **Act** means the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), as amended.

1.2. **IPC** means the Information and Privacy Commissioner of Ontario.

1.3. **Privacy Breach** means when personal information is collected, retained, used, or disclosed in ways that are not in accordance with the privacy provisions of the Act.

1.4. **Response Protocol** means The Corporation of the Town of Whitby's (the "**Town**") official procedure for responding to a Privacy Breach. The rules outline in the protocol are designed to help mitigate the negative effects of the incident.

1.5. **Response Team** means the Town's staff designated to respond to the Privacy Breach and perform the set of actions defined in the Response Protocol.

1.6. **Significant Breaches** are those that have a potential real risk of significant harm. These breaches may involve sensitive personal information, affect a large number of individuals, or are difficult to contain.

2. Responsibilities

2.1. It is the responsibility of the Town to contain and respond to incidents involving unauthorized disclosure of personal information.

2.2. Chief Administrative Officer (the "CAO") to:

a) Decide if matter should be reported to Council.

2.3. Town Clerk, Director of Legislative Services to:

a) Notify the CAO, Town Solicitor, and Risk Management and Insurance Analyst when required; and,

b) Direct the Manager, Information & Content Services on the notification to the IPC.

2.4. Manager, Information & Content Services to:

a) Ensure that the Response Protocol is implemented;

b) Establish Response Team;

c) Inform affected individuals, if required, and respond to questions or concerns;

d) Obtain all available information about the nature of the Privacy Breach and determine the course of events that caused the breach;

e) Ensure details of the Privacy Breach and corrective actions are documented;

f) Notify the Town Clerk, Director of Legislative Services when a breach is reported;

g) Notify the IPC if a Significant Breach occurs; and,

h) Where applicable, work with Corporate Communications to create and distribute messaging.

2.5. Department Heads to:

a) Work with the Office of the Town Clerk by supporting efforts to manage the Privacy Breach by providing staff and financial resources as required.

2.6. Managers and Supervisors to:

a) Alert the Manager, Information & Content Services of a Privacy Breach and work to implement the Response Protocol; and,

b) Inform their Department Head.

2.7. Legislative Specialist, Information & Privacy to:

a) Assist the Manager, Information & Content Services with any activities listed in Section 2.4, as required.

2.8. Technology and Innovation Services Staff to:

a) Assist in the identification, notification, and containment of a Privacy Breach when required (e.g., cyber incidents).

2.9. All Town Staff to:

a) Be alert to the potential for personal information to be compromised, and play a role in identifying, notifying, and containing a Privacy Breach;

b) Notify the Department Head/Manager/Supervisor, or, in their absence, the Manager, Information & Content Services, upon becoming aware of a Privacy Breach; and,

c) Where possible, contain the Privacy Breach by suspending the process or activity that caused the breach and making efforts to retrieve/delete the breached information. This is to be determined on a case-by-case basis.

3. Privacy Breach

3.1. The most common breaches of personal privacy are the unauthorized disclosure of personal information, contrary to Section 32 of the Act. Types of breaches include, but are not limited to the following:

a) Lost or misplaced files;

b) Lost or stolen electronic devices, such as laptops, tablets, and smartphones;

c) Inadvertent disclosure of personal information through human error (i.e., misdirecting an email); and,

d) Cyber incidents.

4. Response Team

4.1. Upon notification of a suspected or confirmed Privacy Breach, the Manager, Information & Content Services will establish a Response Team which may include:

a) Legislative Specialist(s), Information & Privacy;

b) Town Clerk/Director of Legislative Services;

c) Department Head(s) of affected department(s);

d) Staff of affected department(s); and,

e) Staff of other department(s) where appropriate (e.g., Communications, TIS, and Human Resources).

5. Response Protocol

5.1. Identify and Alert

a) When a Privacy Breach is suspected to have occurred, Town staff identify the suspected source of the Privacy Breach and notify the Department Head, Manager, or Supervisor within the department where the Privacy Breach has occurred.

b) The Department Head/Manager/Supervisor shall immediately notify the Manager, Information & Content Services of the Privacy Breach. If the Department Head/Manager/Supervisor is not available, Town staff will directly contact and notify the Manager, Information & Content Services of the Privacy Breach.

c) The Manager, Information & Content Services and the Response Team will attempt to establish the particulars of the Privacy Breach, including:

- The location and date of the Privacy Breach and discovery;

- The technology/application(s) affected;
- 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 associated with the Privacy Breach;
- Any identifiable records associated with the Privacy Breach;
- Any actions already undertaken to contain the Privacy Breach; and,
- Other organizations who have been notified (e.g., police).

5.2. Contain

The Manager, Information & Content Services and the Response Team will undertake the following actions to contain the Privacy Breach:

a) Identify the scope of the Privacy Breach and take steps to contain it;

b) Immediately isolate any physical or system resource that may contain evidence (e.g., paper files, workstations, logs, electronic records, emails, etc.);

c) Suspend any process that caused the Privacy Breach if further breaches are continuing;

d) Retrieve the hard copies of any personal information that has been disclosed;

e) 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,

f) Determine whether the Privacy Breach would allow unauthorized access to any other personal information (e.g., an electronic information system) and take whatever necessary steps are appropriate (e.g., change passwords, identification numbers and/or temporarily shut down a system).

In the event of a cyber incident, Technology and Innovation Services staff will undertake actions outlined in their Cyber Incident Response Plan. Technology and Innovation Services staff will coordinate with the Manager, Information & Content Services to align efforts with the Response Protocol outlined in this procedure.

5.3. Notify

a) The Manager, Information & Content Services shall notify the individuals whose privacy was at risk in the event of a Significant Breach. If law enforcement is involved, ensure that notification will not interfere with any investigations. The notification should be documented, occur by telephone or in writing, and shall include the following information:

- Date of the Privacy Breach;
- Details of the extent of the Privacy Breach;
- The specifics of the personal information at issue;
- Advise of the steps that have been taken to address the Privacy Breach, both immediate and long-term;
- Contact information of the Town and IPC for further information; and,
- A statement that they have a right to make a complaint to the IPC and how to do so.

b) The Manager, Information & Content Services shall ensure appropriate staff are immediately notified of the Privacy Breach.

c) The IPC should be notified of Significant Breaches, such as those that may involve sensitive personal information, those affecting a large number of individuals, or when the Response Team are having difficulties containing the breach. In these situations, the IPC should be notified as soon as reasonably possible.

5.4. Investigate

a) The Manager, Information & Content Services shall conduct an internal investigation into the Privacy Breach.

b) The Manager, Information & Content Services shall ensure the following:

- Containment and appropriate notification have been addressed;
- Review the circumstances surrounding the breach; and,
- Review the adequacy of existing policies and procedures in protecting personal information, Privacy Breach response plans, and staff training.

5.5. Follow Up and Mitigate

a) In cases involving Significant Breaches, a Privacy Breach incident report shall be prepared by the Manager, Information & Content Services outlining the results of the investigation, including any

recommendations to mitigate future incidents. A copy of the Privacy Breach incident report shall be forwarded to the IPC.

b) The CAO shall determine if notification to Council of the Privacy Breach incident report is required.

Original Approved and Signed.

Matthew Gaskell, Chief Administrative Officer, x2211

June 2, 2023

Date