County of Peterborough
Procedure

Procedure No.:	CORP-15-PR01
Subject:	Privacy Breach Procedure
Relates to Policy No.:	CORP-15 Privacy Policy
Approving Manager/Director:	Sheridan Graham, Director, CPS
Date Approved:	June 8, 2020
Approving Director/Team:	Leadership Team
Date Approved:	June 25, 2020

Procedure:

When a privacy breach is alleged to have occurred, County employees shall undertake immediate action in accordance with the Information and Privacy Commissioner of Ontario's 'Privacy Breaches – Guidelines for Public Sector Organizations' attached hereto as Appendix B.

In all instances of a privacy breach or alleged breach the following procedure, conducted in quick succession, or concurrently, shall be followed.

Step 1: Identify and Alert
If a complaint has been received or you suspect that a privacy breach has occurred, contact the Clerk or designate immediately. The Clerk will then investigate the validity of the complaint or suspicion. The "Risk Assessment Chart," attached hereto as Appendix C, can be used to assist in determining if a privacy breach occurred. If a privacy breach is confirmed, the Clerk or designate will assess the severity of the breach and proceed accordingly.

The Clerk or designate shall handle all inquiries with respect to privacy breaches and the actions of the County in response to an alleged or confirmed breach. The Clerk or designate will 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.

Step 2: Contain
The Clerk shall, in cooperation with other employees, carry out the following actions to contain the alleged privacy breach:

- determine what personal information is involved;
- where appropriate and conditional on circumstances, isolate and suspend access to any system associated with the alleged breach (i.e. an electronic information system, change passwords, etc.);

- suspend processes or practices which are believed to have served as a source for the alleged breach;
- take corrective action to:
  - ensure no personal information has been retained by an unauthorized recipient and get their contact information for any future follow up
  - ensure the breach does not allow other unauthorized access to personal information. eg. change passwords, or temporarily shut down a system
  - in a case of unauthorized access by a member of Council or an employee, consider suspending their access rights or appropriate discipline; and
  - retrieve hard copies of any personal information that has been disclosed; and
- take any other action necessary to contain the alleged breach.

Step 3: Notify
The Clerk shall advise the Information and Privacy Commissioner of Ontario of significant breaches, such as those that may involve sensitive personal information or large numbers of individuals, or when having difficulties containing the breach.

The Clerk shall notify all individuals affected by a privacy breach as soon as possible if it is determined that the breach poses a real risk of significant harm to the individual. The Clerk will take into consideration the sensitivity of the information and whether it is likely to be misused.

Notification to individuals should be direct, such as telephone, email or in person, along with a formal letter that includes the following information:

- details of the extent of the breach and the specifics of the personal information that was compromised;
- the steps taken and planned to address the breach, both immediate and long term;
- if the information is financial, a suggestion to contact their bank, monitor their bank and credit card activity and obtain a copy of their credit report;
- contact information for the Clerk (or designate) for information and assistance; and
- a statement that they have a right to make a complaint to the Information and Privacy Commissioner and how they can do so.

Step 4: Investigate
After all efforts have been exhausted to contain the alleged privacy breach and notifying the affected individuals, the Clerk or designate shall undertake an investigation in an attempt to establish:

- identify and analyse the events that led to the breach;
- a timeline of the events that led to the breach and the nature and sensitivity of the personal information disclosed the nature;
- the source of the breach, including any policies or procedures responsible for the breach. Review policies and practices in protecting personal information, privacy breach response plans and employee training to determine whether changes are needed;
- take corrective action to prevent similar breaches in the future and ensure employees are adequately trained; and

- any other factors relevant to the circumstances.

Step 5: Report and Follow-Up
Following the completion of the investigation, a report shall be prepared by the Clerk or designate outlining the results of the investigation, including any recommendations to mitigate future incidents. If the Information and Privacy Commissioner was notified, a copy of the report shall be sent to them. A copy of the report to all individuals who were affected by the privacy breach.

The report will also be included on the Council of the County of Peterborough Agenda when:

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

Any recommendations from the report will be reviewed and where appropriate, implemented.

Review Cycle:

These procedures will be reviewed at least once per term of Council with the review of Policy No. CORP-15.