Waterloo Region District School Board

Administrative Procedure 1104
PRIVACY BREACH PROTOCOL

PROTOCOL

Responsibility:	Director of Education Freedom of Information, Privacy and Records Information Management Officer
Legal References:	*Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* *Personal Health Information Protection Act (PHIPA) O.Reg 329/04* *Personal Information Protection and Electronics Documents Act*
Related References:	Board Policy 1014 - Privacy Protection and Access to Information Board Policy 1015 - Records Information Management *Administrative Procedure 1100 - Privacy Protection and Access to Information* *Administrative Procedure 1110 - Records Information Management* *Administrative Procedure 4060 - Board E-Mail Protocol*
Revisions:	June 2020
Reviewed:	August 2016, June 2020

1. Preamble

1.1 The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) establishes rules for government organizations to follow to ensure the protection of individual privacy. A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with MFIPPA.

A privacy breach occurs when personal information is collected, used, disclosed, lost or stolen, retained, or destroyed in a manner inconsistent with privacy legislation. Personal information can be compromised in many ways. Some breaches have relatively simple causes and are contained, while others are more systemic or complex.

Privacy breaches are often the result of human error; such as an individual's personal information sent by mistake to another individual. A breach can be more wide-scale, such as when a computer program change causes the personal information of many individuals to be compromised through inadvertent distribution.

A security incident is "a violation or threat of violation of computer security policies, acceptable use policies or standard security practices". When a security incident involves personal information it would then be escalated to a privacy breach.

1.2 Personal information can be compromised in many ways. Some breaches have relatively simple causes and are contained, while others are more systemic or complex.

Examples of privacy breaches include:

- leaving student or staff personal information on a desktop or in a photocopier and a parent or student finds the information;
- leaving a computer "open" (i.e. not logged out or not locked) and a parent, member of the public or a student is able to view personal information;
- throwing confidential information in a recycle bin or garbage container;
- sending an email to the wrong group of recipients;
- a security incident that compromises personal or sensitive information.

2. General

2.1 If a privacy breach, or suspected privacy breach has occurred, Board staff, upon learning of the breach or suspected breach shall immediately take the following actions:

1. Contain the breach to stop any more information from being revealed
2. Notify your immediate supervisor
3. Involve the Freedom of Information, Privacy and Records Information Management Officer
4. Complete the *Privacy Breach Investigation Report* form (IS-11-D).

3. Containment

3.1 The first step in responding to a privacy breach is to stop the inappropriate flow of data. This may include such actions as taking down a website; retrieving items from garbage bins; "unsending" an email message (although messages cannot be recalled from Smartphone); calling a recipient and asking them to destroy the information; changing a password; etc. Record the names and contact information of any persons that received inappropriate information, in case there is a need for later follow-up.

3.2 Involve the Freedom of Information, Privacy and Records Information Management Officer to ensure all containment efforts are in place.

3.3 Document breach and containment activities

4. Investigate

4.1 Once the breach is contained the assessment, investigation into the breach needs to take place and include the Freedom of Information, Privacy and Records Information Management Officer

4.2 Assess the extent of the breach. In order to assist staff investigate the breach, staff should ask themselves the following questions:

- "What data was revealed?"
- "How much data was revealed?"
- "How sensitive was the data?"
- "How long has the data been inappropriately available?"
- "Has the data been reviewed and/or used?", and
- "How did the breach happen?" will help staff investigate the breach

4.3 Evaluate the risk, what was exposed and the cause of the breach.

4.4 Determine if the breach was benign (human error, accidental), or malicious (deliberate, hacking). Note if it was a systemic breach (e.g., network security failure), or an isolated incident (e.g., lost folder).

4.5 Find out who was affected (i.e., whose personal information was involved, how many people)**.**

4.6 Determine if the data could be used for fraudulent or otherwise harmful purposes (e.g., identity theft; access to systems/devices; public humiliation).

5. Implement Change

5.1 In response to a privacy breach, the Freedom of Information (FOI) Office will determine in collaboration with the affected departments if changes to existing policies, procedures, and practices are required to prevent a similar breach in the future. The FOI Office will complete the following steps.

5.1.1 Review existing policies, procedures and practices for managing and safeguarding personal information;

5.1.2 Review employee training on policies and procedures related to security and privacy; and
5.1.3 Recommend a course of action to remediate the situation.

6. Notifying affected parties

6.1 Based on the level of risk and the type of information breached, determine whether to notify individuals and provide information. As assessment of risk should encompass a review of the following:

- risk of identity theft
- risk of physical harm
- risk of harm, humiliation or damage to reputation
- legislative requirements

6.2 Depending on the nature of the breach, the Freedom of Information, Privacy and Records Information Management Officer may also notify the Ontario Information and Privacy Commissioner's Office, who may launch their own investigation.

6.3 In cases where the breach involves personal health information, the Freedom of Information, Privacy and Records Information Management Officer may be required to notify the Ontario Information and Privacy Commissioner's Office.