

<b>TOPIC:</b>	<b>Privacy Breach Protocol</b>
<b>EFFECTIVE:</b>	<b>May 2010</b>
<b>CROSS-REFERENCE:</b>	<b>Municipal Freedom of Information &amp; Protection of Personal Privacy Halton District School Board Privacy and Information Policy Related Halton District School Board procedures</b>
<b>REVISION DATE:</b>	<b>September 2012</b>
<b>RESPONSIBILITY:</b>	<b>Superintendent of Education (Privacy &amp; Information Management) Privacy &amp; Information Management Champion Freedom of Information Coordinator</b>

**INTENT STATEMENT**

The Halton District School Board is committed to the protection of personal information under its control and to the individuals' right of privacy regarding personal information that is collected, used, disclosed, and retained in the school system.

While protection of this information is paramount, and is the priority of the Halton District School Board, the Board recognizes unintentional breaches can occur. To that end, the following procedures outline the immediate actions to be undertaken by the Halton District School Board in the case of a privacy breach.

**PROCEDURES**

Under the *Municipal Freedom of Information and Protection of Privacy Act*, the boards of trustees of Ontario school boards/authorities are responsible for personal information under their control and may designate an individual within their school board/authority who is accountable for compliance with privacy legislation.

Under the *Personal Health Information Protection Act*, health information custodians are responsible for personal health information and may designate an individual within their school board as an agent to assist with compliance with privacy legislation.

A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the *Acts*.

Among the most common breaches of personal privacy is the unauthorized disclosure of personal information, contrary to Section 32 of the municipal *Act*. For example, personal information may be lost (a file is misplaced within an institution), stolen (laptop computers or electronic devices are prime examples), or inadvertently disclosed through human error (sensitive information is left in areas accessible to others, such as a photocopier or fax; or a letter addressed to person "A" is actually mailed to person "B").

Upon learning of a privacy breach, immediate action must be taken.

The following list is in no way meant to be inclusive of all potential breaches, but instead provide examples of types of breaches and expected responses:

***Staff should contact their principal, supervisor or manager in these breach situations:***

- loss of student work (essays, marked documents)
- loss of markbooks, attendance books with personal information
- loss of photos with identification

***Principals, supervisors and/or managers should contact their superintendent in situations related to these breaches:***

- staff personal data resulting in privacy issues
- Ontario Student Records (OSR)
- medical, financial or personnel records
- student custodial and/or guardian issues

The following containment practices should be followed subsequent to any potential breach:

***Containment:***

- identify the scope of the potential breach
- retrieve copies of any personal information;
- ensure 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 follow-up is required;
- determine whether the privacy breach would allow unauthorized access to any other personal information (ie: an electronic information system), and take whatever necessary steps are appropriate (ie: change passwords, identification numbers, and/or temporarily shut-down a system).

The Superintendent, in consultation with the Principal will then notify the Board's Freedom of Information manager. The Superintendent and FOI manager will coordinate to complete the following steps (simultaneously or in quick succession), and work with the Information and Privacy Commission (IPC) in seeking resolution to the matter as appropriate.

***Notification: use of the IPC's "Breach Notification Assessment Tool" must occur***

- notify the individuals whose privacy was breached, by telephone or in writing;
- provide details of the extent of the breach and the specifics of the personal information at issue;
- if financial information, or information from government-issued documents are involved, include the following in the notice:

*As a precautionary measure, we strongly suggest you contact your bank, credit card company, and appropriate government departments to advise them of this breach.*

*You should monitor and verify all bank accounts, credit card and other financial transaction statements for any suspicious activity.*

*If you suspect misuse of your personal information, you can obtain a copy of your credit report from a credit reporting bureau to verify the legitimacy of the transactions listed.*

*Equifax at 1-800-465-7166 or [www.equifax.ca](http://www.equifax.ca)*

*TransUnion at 1-800-663-9980 or [www.tuc.ca](http://www.tuc.ca)*

*If you are concerned you may be a victim of fraud, you may request these organizations to place a fraud alert on your credit files instructing creditors to contact you before opening any new accounts.*

*You may also wish to review the publication of the Information and Privacy Commissioner of Ontario entitled "Identify Theft: How to Protect Yourself", at [www.ipc.on.ca](http://www.ipc.on.ca)*

- advise of the steps that have been taken to address the breach, both immediate and long-term;
- advise the individual(s) that the IPC has been contacted to ensure all obligations under the Act are fulfilled.

***Additional Steps:***

- conduct an internal investigation into the matter, linked to the IPC's investigation, to:
  - ensure the immediate requirements of containment and notification have been addressed;
  - review the circumstances surrounding the breach;
  - review the adequacy of existing policies and procedures in protecting personal information;
  - address the situation on a systemic basis, determining if program-wide or institution-wide procedures may warrant review
  - advise the IPC of any findings, and work cooperatively to make necessary changes; and
  - ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of the Act