Topic:	**Privacy Breach Protocol**
Effective:	**May 2010**
Cross-Reference:	**Halton District School Board Privacy and Information Policy; *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c.M.56; *Personal Health Information Protection Act*, S.O. 2004, c.3, Sched. A; *Education Act*, R.S.O. 1990, c.E.2.**
Revision Date:	**December 2014, January 2020**
Review Date:	**December 2023**
Responsibility:	**Superintendent of Education - Information Services**

INTENDED PURPOSE:
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.

SCOPE
This Administrative Procedure applies to all Personal Information as defined by MFIPPA as well as all Personal Health Information as defined by PHIPA that is within the custody and control of the Board.

PROCEDURES
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* (see cross references above).

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), or inadvertently disclosed through 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.

Managing a Privacy Breach
A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information (PI) or personal health information (PHI). Such activity is "unauthorized" if it occurs in contravention of MFIPPA or, if applicable, a relevant provision of PHIPA.

An example of a privacy breach would be personal, or personal health information becoming lost or stolen or personal information being mistakenly emailed to the wrong person.

The recommended privacy breach incident protocol has five steps. Step 1 is the responsibility of the individual or individuals who first become aware of the potential breach. The second through fifth steps are the responsibility of the Manager, Privacy and Records, working in cooperation with other school board officials and school staff, as necessary.

Step 1: Identifying and Reporting the Breach
Any employee who becomes aware of a possible breach of privacy involving personal or personal health information in the custody or control of the school or school board or one of its employee Health Information Custodian (HIC) will immediately inform their immediate supervisor, who will verify the circumstances of the breach to the extent possible and, if satisfied that a breach has or may have occurred, will contact the Manager Privacy and Records.

Prompt investigation and notification to the Manager, Privacy and Records is essential to the resolution of the breach.

The Manager, Privacy and Records, in consultation with the appropriate board staff, will decide whether or not to proceed with the breach protocol while taking into consideration the seriousness and scope of the breach and any other relevant considerations.

When a breach has been confirmed, the Manager, Privacy and Records will implement the remaining steps of the privacy breach protocol and invoke the HDSB Incident Response Plan as needed.

Step 2: Containing the Breach
The Manager, Privacy and Records will take the following steps, as appropriate, to limit the scope and effect of the breach:

1. Work with staff to immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached,
2. or correcting weaknesses in security, and

In consultation with relevant Board officials, coordinate notification of the police if the breach involves, or may involve, any criminal activity.

Step 3: Evaluating the Risks Associated with the Breach
To determine what other steps are immediately necessary, the Manager, Privacy and Records, working with other Board staff as necessary, will assess the risks associated with the breach. The following factors will be among those considered in assessing the risks:

1. Personal information involved
   a. What data elements have been breached? Generally, the more sensitive the data, the higher the risk. Health information, social insurance numbers and financial information that could be used for identity theft are examples of sensitive personal information.
   b. What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?

2. Cause and Extent of the Breach
   a. What is the cause of the breach?
   b. Is there a risk of ongoing or further exposure of the information?

c. What is the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
d. Is the information encrypted or otherwise not readily accessible?
e. What steps have already been taken to minimize the harm?

3. Individuals Affected by the Breach
   a. How many individuals are affected by the breach?
   b. Who was affected by the breach: employees, students, alumni, retirees, public, contractors, clients, service providers, other individuals/organizations?

4. Foreseeable Harm from the Breach
   a. Is there any relationship between the unauthorized recipients and the data subject?
   b. What harm to the individuals will result from the breach? Harm that may occur includes:
      i. Security risk (e.g., physical safety)
      ii. Identity theft or fraud
      iii. Loss of business or employment opportunities
      iv. Hurt, humiliation, damage to reputation or relationships
   c. What harm could result to the Board as a result of the breach? For example:
      i. Loss of trust in the Board, or school
      ii. Loss of assets
      iii. Financial exposure
   d. What harm could result to the public as a result of the breach? For example:
      i. Risk to public health
      ii. Risk to public safety

Step 4: Notification

Notification can be an important mitigation strategy in the right circumstances. The key consideration overall in deciding whether to notify will be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed. The Manager, Privacy and Records will work with the staff involved and the appropriate Board officials to decide the best approach for Notification.

1. Notifying Affected Individuals
   Some considerations in determining whether to notify individuals affected by the breach include:
   a. Contractual obligations require notification.
   b. A risk of identity theft or fraud (usually because of the type of information lost, such as SIN, banking information, identification numbers).
   c. A risk of physical harm (if the loss puts an individual at risk of stalking or harassment).
   d. A risk of hurt, humiliation or damage to reputation (for example when the information lost includes medical or disciplinary records).

2. When and How to Notify
   a. When: Notification of individuals affected by the breach will occur as soon as possible following the breach. However, if law enforcement authorities have been contacted,

those authorities will assist in determining whether notification will be delayed in order not to impede a criminal investigation.

b. How: The preferred method of notification is direct - by phone, letter or in person - to affected individuals. Indirect notification - website information, posted notices, media - may also be used. Using multiple methods of notification in certain cases may be the most effective approach.

3. What will be Included in the Notification?
   Notifications will include the following pieces of information:
   a. Description of the breach
   b. Description of the information inappropriately accessed, collected, used or disclosed.
   c. The steps taken to mitigate the harm.
   d. Next steps planned and any long term plans to prevent future breaches.
   e. Steps the individual can take to further mitigate the risk of harm.
   f. Contact information for the Manager, Privacy and Records or other school board official such as the Principal/Supervisor.

4. Others to Contact
   Regardless of what obligations are identified with respect to notifying individuals, notifying the following authorities or organizations will also be considered:
   a. Police: if theft or other crime is suspected.
   b. Insurers or others: if required by contractual obligations.
   c. Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies.
   d. Applicable research ethics authority
   e. Office of the Information and Privacy Commissioner (OIPC): The following factors are relevant in deciding when to report a breach to the OIPC:
      i. the sensitivity of the personal information;
      ii. whether the disclosed information could be used to commit identity theft;
      iii. whether there is a reasonable chance of harm from the disclosure including non pecuniary losses;
      iv. the number of people affected by the breach; and
      v. whether the information was fully recovered without further disclosure.

Step 5: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, the Manager, Records and Privacy will further investigate the cause of the breach as necessary. As a result of this evaluation, the Manager, Records and Privacy will assist the responsible staff to put into effect adequate long-term safeguards against further breaches such as assisting with the implementation of appropriate technical, physical or administrative safeguards designed to prevent any subsequent breach of personal information.