HWDSB

PROCEDURE FOR POLICY 1.6

PRIVACY BREACH RESPONSE PROCEDURE

RATIONALE:

As an accountable organization, Hamilton-Wentworth District School Board (HWDSB) is committed to protecting the personal information entrusted to it and continually improving its information handling practices.

Safeguarding personal information, as well as observing privacy standards for the collection, use, disclosure, retention, and destruction of personal information, are key to good data stewardship.

Accountable organizations recognize that data breaches do occur and they strive to be prepared by implementing data breach response plans, by keeping track of breaches and their root causes, and by identifying patterns and trends to inform positive change.

Accountable school boards are prepared to respond to breaches and minimize the impact on their communities which, in turn, protects and fosters the trust relationship at the core of public service.

The following privacy breach response has been developed to ensure that every breach, no matter how small, is handled professionally and is used as an opportunity to improve what we do.

TERMINOLOGY:

Privacy Breach: Occurs when there is an unauthorized release of or access to personal information. In other words, personal information is seen by or is in the custody/control of people who do not have the legal authority to access it (e.g., on a laptop that is stolen, in an email sent to the wrong person, on a paper that is lost, turned over to third parties without legal authority, notice, or consent). Breaches can be intentional or accidental.

Personal Information: Any information about an identifiable individual. In other words, any information about someone that could alone, or in combination with other information, lead to someone being identified (e.g., name, race, ethnicity, age, gender, sexual orientation, image/photograph, marital or family status, achievement data, education level, medical/psychiatric/criminal/employment history, health status or treatment, financial transactions, OEN, address, telephone number, S.I.N., health number, even personal opinions and views).

Record: Refers to any documented information in any format, including print, film or electronic, that is in the custody and/or control of the organization (e.g., email correspondence, memos, plans, maps, drawings, diagrams, pictures, graphic work, photographs, videos, microfilm, sound recording, machine readable records, and any other documentary material).

PRIVACY BREACH RESPONSE PROCEDURE

PROCEDURES:

The *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA) and the *Personal Health Information Protection Act* (PHIPA) set out rules that persons or organizations must follow when collecting, using, disclosing, retaining, and disposing of personal information.

These Acts balance the rights of individuals to their privacy, with the legitimate needs of staff in organizations to collect, use and share information to conduct their work.

These Acts also require organizations to take reasonable steps to ensure that information in their custody or control is protected against theft, loss, unauthorized use or disclosure, modification, or disposal.

When a staff member becomes aware of a privacy breach, timely assistance and remedial steps are vital to minimizing harm, while demonstrating accountability and restoring trust.

HWDSB's Privacy Breach Response includes the following steps:

1.0 Respond

1.1 Respond immediately by notifying the appropriate supervisory staff and the Privacy Officer.

2.0 Contain

2.1 Identify the scope of the potential breach and take steps to contain it.

2.2 Retrieve the information if the records are in hard copy.

2.3 Ensure that no copies were made by whomever had access to the information.

2.4 Obtain contact information of the authorized person/party in case follow-up is needed.

2.5 Determine if this breach would allow further unauthorized access, (e.g., via an electronic information system), to information and take whatever steps are necessary to prevent it (e.g., change passwords, temporarily shut down a system).

3.0 Investigate

3.1 Evaluate the risk of the exposure and the cause of the breach.

3.2 Determine if the breach was benign (human error, accidental), or malicious (deliberate sabotage, hacking).

3.3 Note if it was a systemic breach (e.g., network security failure), or an isolated incident (e.g., lost folder).

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

3.5 Determine what types of data were involved and how sensitive it is (e.g., age & gender vs. medical information).

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

4.0 Notify

4.1 Based on the level of risk and the type of information breached, determine whether to notify individuals and provided information.

4.2 Determine the best method to notify individuals (e.g., telephone or in writing). This will depend on the circumstances (i.e., risk, exposure, sensitivity).

4.3 Provide details to individuals of the extent of the breach and type of data.

4.4 Advise individuals of the steps that were taken immediately following the breach and what steps will be taken in the future.

4.5 Apologize to individuals whose personal information was breached while in our custody.

5.0 Change

5.1 Review the circumstances surrounding the breach. Ensure the immediate requirements of containment and notification have been addressed.

5.2 Identify changes in practice that could prevent a similar breach.

5.3 Identify any systemic practices or procedures that warrant review.

5.4 Work to implement necessary changes to reduce risk.

5.5 Ensure staff are properly trained in new safeguards.

5.6 Document the details of the breach and the breach response.

PRIVACY BREACH RESPONSE PROCEDURE

6.0 Responsibility

6.1 All Employees

6.1.1 All HWDSB employees need to be alert to the potential for personal information to be out-of-place. Employees play a vital role in identifying, notifying, containing, and remediating a breach.

6.1.2 In case of a breach or suspected breach, employees must notify their supervisor and/or the Privacy Officer at once.

6.1.3 Work with staff and Privacy Officer to implement the breach response protocol.

6.2 Superintendents, Managers, and Principals

6.2.1 Alert the Director of Education or Privacy Officer of a breach or suspected breach.

6.2.2 Work with staff and Privacy Officer to implement the breach response protocol.

6.3 Director of Education

6.3.1 Brief senior management and trustees as necessary and appropriate.

6.3.2 Review internal investigation reports and approve required remedial action.

6.3.3 Monitor implementation of remedial action and ensure that all five steps of the breach response protocol are followed.

6.4 Privacy Officer

6.4.1 Work with affected staff to implement the breach response protocol.

6.4.2 Ensure that all five steps of the breach response protocol are implemented and make recommendations for remediation.

6.4.3 Provide a report to senior administration on the progress and outcome of the breach response and where appropriate, report the breach to the Office of the Information and Privacy Commissioner of Ontario.

6.4.4 Track privacy breaches and details of breach responses.

6.4.5 Determine when notifications are applicable and ensure they are sent.

6.4.6 Promote changes in practice that reduce breach risk and monitor the implementation of changes.