Section:	District Administration	
Title:	Privacy Breach Management	2.4.6

Purpose
To outline the procedures to follow after a privacy breach event.

Definitions
A privacy breach occurs when personal information is compromised when it is collected, used, disclosed, retained or destroyed in a manner that is inconsistent with the privacy legislation, and Mission Public Schools' privacy policies and procedures.

Guidelines
A. All employees are responsible for:
   a) Understanding the importance of protecting personal information under the custody and control of the school district from misuse or disclosure contrary to the legislation or the purpose for which the personal information is collected.
   b) Identifying a breach or a potential breach and immediately notifying their supervisor, or in the absence of their supervisor, the school district's privacy officer or privacy coordinator.
   c) Immediately containing the breach by:
      i. suspending the process/activity that caused the breach,
      ii. collecting breached documents if possible, and
      iii. or any other appropriate action to contain the breach.

B. Principals, Managers and Directors are responsible for:
   a) Notifying the privacy officer of the breach.
   b) Obtaining all the available information about the breach and completing the Privacy Breach Checklist.
   c) Working with the involved employees and privacy officer to contain the breach and document corrective measures.

C. Privacy Officer
   a) Ensuring all steps of the response procedure are implemented.
   b) Supporting the principal or the supervisor in responding to the breach.
   c) Reviewing internal reports
   d) Approving and monitoring required remedial action.
   e) Notifying the Office of the Privacy Commissioner if appropriate.

Procedures
1. Contain and Control
   i. Identify the scope of the breach and contain it. Containment means taking immediate action to put an end to unauthorized use or access to personal information.
   ii. Document the breach and activities taken to contain the breach. Prepare a thorough record of all actions taken, following the Privacy Breach Checklist.
   iii. Notify the organization's privacy officer and the information technology department if the breach involves electronic information. Determine if others within the school district need to be made aware of the incident and discuss it with the privacy officer.

iv. Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or that will allow you to take appropriate corrective action.

2. Evaluate the risks
   i. Determine what information was compromised.
   ii. Determine who and how many individuals are affected by the breach.
   iii. Determine the possible risks of the use of personal information.

3. Notification
   i. Notification should occur as soon as possible following the breach; refer to the Notification Resource Document.
   ii. Determine if the notification is required and who should be notified. Review with the privacy officer if uncertain.
   iii. Determine if there are contractual obligations that require notification.

4. Mitigation and Prevention
   i. The principal, manager, or director, with the assistance of the privacy officer or the information technology department as necessary, is to investigate the cause of the breach thoroughly and consider a detailed prevention plan.
   ii. The privacy officer will determine remedial actions that need to be implemented.
   iii. Corrective measures and consequences must be determined on a case-by-case basis.
   iv. Evaluate, develop, or improve necessary long-term safeguards against a future breach, including an action plan to minimize the risk of a future breach.

Date Approved: February 2023

Legal Reference: *Access to Information and Protection of Privacy Act*

Cross Reference: *Access to Information and Protection of Privacy and Personal Information Policy*

Privacy Management Program (includes procedures 2.4.1 to 2.4.7)

Forms: *Privacy Breach Checklist*