Medicine Hat Public School Division

601-1st Avenue SW, Medicine Hat, AB T1A 4Y7 | Phone 403.528.6700 | Fax 403.529.5339 | www.mhpsd.ca

MEDICINE HAT PUBLIC BOARD OF EDUCATION OPERATES AS MEDICINE HAT PUBLIC SCHOOL DIVISION,
AND FOR THE PURPOSE OF THIS DOCUMENT WILL BE REFERRED TO AS "MHPSD" AND/OR "DIVISION"

SECTION 400 – Business Administration

ADMINISTRATIVE PROCEDURE: LOGGING AND AUDITING

PROCEDURE CODE:	*412 AP 005*
Policy Reference: Policy 412: Managing Division Information, Access, And Privacy Policy	

PURPOSE

The purpose of this policy is to establish requirements for logging, monitoring, and auditing activities within the Division to ensure the protection of personal information in accordance with the Protection of Privacy Act (POPA), specifically section 10(1), requiring reasonable security arrangements.

SCOPE

This procedure applies to all employees, contractors, volunteers, students, and service providers acting on behalf of MHPSD who collect, use, disclose, or manage information under the custody or control of the organization.

PROCEDURE

MHPSD shall ensure that all access to and activity within the Division IT programs are appropriately logged, monitored, and auditable.

1. Logging practices must support:
   1.1. Detection of unauthorized access or misuse
   1.2. Investigation of privacy incidents
   1.3. Compliance with POPA and Division policies
   1.4. Accountability for access to sensitive personal information
   1.5. Access to logs shall be restricted to authorized personnel and used only for legitimate operational, security, or compliance purposes.

2. Logging requirements include:
   2.1. User logins and logouts
   2.2. Failed login attempts
   2.3. MFA events (where applicable)
   2.4. Session duration and timestamps
   2.5. Data Access and Modification
      2.5.1. Viewing of student data (where technically available)
      2.5.2. Creation, modification, or deletion of student records
      2.5.3. Updates to sensitive fields
   2.6. Administrative Activity
      2.6.1. Changes to user roles and permissions
      2.6.2. Configuration changes
      2.6.3. Data imports and exports
      2.6.4. Integration activity
   2.7. Vendor Access
      2.7.1. All vendor support sessions, including duration, scope, and actions taken
3. Monitoring and Review
   3.1. Reactive Monitoring: Logs are reviewed in response to suspected incidents, unauthorized access, or anomalies.
   3.2. Proactive Monitoring: Periodic review of administrative access, privileged accounts, and vendor sessions in alignment with the Privacy Management Program.
4. Access to Logs
   4.1. Access is restricted to Division IT personnel and authorized privacy or security officials.
   4.2. Logs are accessed only for security monitoring, incident investigation, and compliance verification.
   4.3. Unauthorized access or use of logs is prohibited.
5. Retention of Logs
   5.1. Logs are retained in accordance with system capabilities and Division records retention practices.
   5.2. Logs must be retained long enough to support investigations and compliance requirements.
6. Audit Practices
   6.1. Scheduled Audits: Periodic review of user access, administrative accounts, and role assignments.

6.2. Event-Driven Audits: Triggered by incidents, suspicious activity, or regulatory requirements.

6.3. Vendor Access Audits: Review of approvals, session duration, and compliance with the no persistent access requirement.

7. Integration With Privacy Incident Response

7.1. Logging and audit data must support investigation of privacy incidents, Real Risk of Significant Harm (RROSH) assessments, and breach notification processes under POPA.

Approved: May 11, 2026