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: PRIVACY MANAGEMENT PROGRAM

PROCEDURE CODE:	*412 AP 001*
Policy Reference: Policy 412: Managing Division Information, Access, And Privacy Policy	**Exhibits:** 412 E 001 – Delegation of Authority 412 E 002 – Security Classification 412 E 003 – Personal Information Banks

PURPOSE

To establish and maintain a Privacy Management Program (PMP) in compliance with Section 25 of the Protection of Privacy Act (POPA). The PMP ensures the protection of personal information, and non-personal data held by MHPSD.

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

1. MHPSD shall implement and maintain a Privacy Management Program that includes policies, procedures, safeguards, and training to support compliance with POPA and is proportional to the volume and sensitivity of the personal information in the Division's custody or control.
2. A Privacy Officer is designated as the Secretary Treasurer to oversee privacy compliance and the administration of the PMP.
   2.1. Exhibit 412 E 001 – Delegation of Authority
3. MHPSD shall maintain procedures addressing:
   3.1. Correction requests for personal information,
   3.2. Privacy incidents and breach response,
   3.3. Privacy complaints,

3.4. Creation, use, and disclosure of non-personal data (where applicable),
3.5. Use of automated systems involving personal information.

4. Reasonable security arrangements must be implemented to protect personal information, data derived from personal information, and non-personal data, including:
   4.1. Administrative safeguards: policies, procedures, and training,
   4.2. Physical safeguards: protection of facilities and systems from unauthorized access or environmental hazards,
   4.3. Technical safeguards: access controls and system security measures.
5. MHPSD shall maintain a security classification system based on the sensitivity of personal information and data to ensure appropriate protection, retention, and destruction practices.
   5.1. Exhibit 412 E 002 – Security Classification
6. The Division may engage in data matching or the creation of non-personal data (including synthetic data) exclusively for research and analysis or for planning, administering, delivering, or evaluating Division programs and services.
   6.1. For the purpose of data matching, the Division must not collect personal information directly from individuals.
   6.2. For every instance of non-personal data creation, the Division must maintain a record detailing the source information, the method used, the purpose, and a formal assessment ensuring the data prevents re-identification. The Division is prohibited from disclosing data derived from personal information to external parties, unless back to the public body that provided the original information.
   6.3. If the Division discloses non-personal data to a person or entity that is not a public body, there must be a signed agreement.
   6.4. This agreement must explicitly include a prohibition on any actual or attempted re-identification of the data.
   6.5. Data derived from matching may only be used for its original purpose and for as long as reasonably necessary. Once that purpose is met, the data must be destroyed or transformed into non-personal data.
7. Mandatory privacy training is required for all employees and individuals performing services for MHPSD to ensure awareness of privacy obligations and procedures.
8. Personal Information Banks (PIBs) will be made public and updated regularly.
   8.1. Exhibit 412 E 003 – Personal Information Banks
9. Privacy Impact Assessments (PIAs) will be implemented for new or significantly modified programs, systems, or services involving personal information.
10. MHPSD will ensure adequate, industry standard monitoring and response systems are in place to protect Division systems that contain personal information. Information only will be

shared with individuals or organizations that have the right of access or the consent of the individual about whom the information applies.

10.1. Proactive monitoring of information systems will actively take place for programs that involve personal information, non-personal data, and derived data to mitigate risks and ensure security measures.

11. Upon request, MHPSD must provide a copy of the Privacy Management Program, or directions on how to access it, within 30 business days, except for technical information that could compromise information security.
12. The Privacy Management Program shall be reviewed every three years to ensure continued compliance with legislative requirements and organizational needs.

12.1. A review may be triggered sooner than three years if there are significant changes in the volume or sensitivity of the data the Division collects.

REFERENCES

Protection of Privacy Act (POPA)

Protection of Privacy (Ministerial) Regulation

Approved: May 11, 2026