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

POLICY 412: MANAGING DIVISION INFORMATION, ACCESS, AND PRIVACY POLICY

BACKGROUND

Medicine Hat Public School Division (MHPSD) is committed to managing records, data and information as an indispensable and strategic resource, consistent with international record and information standards and provincial legislation. This policy ensures that MHPSD fulfills its dual legislative obligations to maintain public accountability and openness required by the Access to Information Act (ATIA), while providing robust protection of personal privacy required by the Protection of Privacy Act (POPA).

POLICY

All records and information collected and created in the service of Medicine Hat Public School Division remain the property of MHPSD. MHPSD is accountable for managing these records and information throughout their entire life cycle.

1. Principles of Access and Accountability
   MHPSD is guided by the core principle that a right of access is the cornerstone of an open, transparent, and accountable public body. MHPSD believes that:
   1.1. Public Right of Access: The public retains the fundamental right of access to Division records and information. This right is maintained, subject only to the limited and specific exceptions explicitly authorized in access legislation set by the ATIA.
   1.2. Openness and Proactive Disclosure: Access requests are considered an addition to, and do not replace existing procedures for accessing information. MHPSD must therefore continue to accommodate requests for information outside of the formal access request process whenever possible, provided such routine disclosures remain consistent with applicable access and privacy legislation.
2. Principles of Privacy Protection
   The Board of Trustees recognizes its responsibility for documenting the activities and results for which MHPSD is accountable, while ensuring the strict protection of individual privacy. MHPSD must control the collection, use, and disclosure of personal information and control the creation, use, and disclosure of information assets, including data derived from personal information and non-personal data.

GUIDELINES

MHPSD records and information management practices and processes shall adhere to the following under the new legislation:

1. Head of Public Body: The Board designates the Superintendent as the Head of the Public Body under section 55 of the Protection of Privacy Act, and under section 1(h) of the Access to Information Act.
2. Designated Authority: The Superintendent shall ensure the implementation of this policy through administrative regulations, including the delegation of duties under access and privacy legislation.
3. Privacy Management Program: Under Section 25 of POPA, every public body must establish and implement a PMP consisting of documented policies and procedures that promote compliance proportional to the volume and sensitivity of the information.
4. Privacy Impact Assessment: All new or significantly changed programs will require the completion of a Privacy Impact Assessment.
5. Employee Compliance: All employees, including contractors and volunteers, must be compliant with POPA, adhering to training requirements and respecting the principles of access to information and protection of privacy.
6. Governance Structure: The Protection of Privacy (Ministerial) Regulation, section 6(1)(a), requires the designation of an Access and Privacy Officer within MHPSD who will be responsible for ensuring compliance with accountability for managing information, and overseeing compliance with access and privacy legislation.
7. Protection of Personal Information: The Division must protect personal information, data derived from personal information and non-personal data by making reasonable security arrangements and provide notification of collection.
8. The Division must ensure information used to make decisions affecting an individual is accurate and complete. Such information must be retained for at least one year to allow the individual a reasonable opportunity to access it.
9. If the Division will use personal information in an automated system to generate content or make decisions, recommendations or predictions, the Division is required, as part of its privacy management program, to establish standards and procedures detailing how automated systems will use personal information, including any required security or technical safeguards that will be implemented to protect the personal information.
10. Mandatory Breach Notification: Section 10(2) of POPA mandates that if a breach occurs (loss, unauthorized access, or disclosure) and a reasonable person would consider there to be a real risk of significant harm to an individual, the Division must notify the affected individual, the Information Commissioner, and the Minister.

11. Data Matching: The Division may engage in data matching and the creation of non-personal (anonymized or synthetic) data for research, analysis, and program evaluation. All data matching must be performed using reasonable security arrangements.
12. The Division will not sell personal information in any circumstances or for any purpose, including for marketing or advertising purposes
13. Whistleblower Protection: No adverse employment action shall be taken against an employee who, in good faith, discloses a contravention of the Act to the Commissioner.
14. Offences and Penalties: Knowing contravention of this policy or the Act, including unauthorized use of data or attempted re-identification, may result in statutory fines for the Division and for the individual.

ADMINISTRATIVE PROCEDURES

412 AP 001 – Privacy Management Program
412 AP 002 – Collection and Correction of Personal Information
412 AP 003 – Privacy Incidents
412 AP 004 – Access to Information
412 AP 005 – Logging and Auditing

ADMINISTRATIVE PROCEDURE - EXHIBITS

412 E 001 – Delegation of Authority
412 E 002 – Security Classification
412 E 003 – Personal Information Banks
412 E 004 – Correction of Personal Information
412 E 005 – Access to Information Fee Schedule

REFERENCES

Access to Information Act (ATIA)
Access to Information Regulations
Protection of Privacy Act (POPA)
Protection of Privacy (Ministerial) Regulation