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 - EXHIBIT: SECURITY CLASSIFICATION

| *EXHIBIT CODE:* | *412 E 002* |
|---|---|
| **Policy Reference:** 412 – Managing Division Information, Access, and Privacy | |

EXHIBIT

DEFINITIONS:

1. Authorized Users: Employees, teachers, administrators, trustees, students, volunteers, contractors, consultants, service providers, and other individuals granted access to Division Information Assets.
2. Information: Data in any format or medium that is collected, created, transmitted, stored, or maintained by the School Division.
3. Information Systems: The Division's technology infrastructure, including networks, devices, software applications, cloud services, and databases.
4. Information Assets: Information and the systems used to store, process, or transmit that information.
5. Information Asset Owner: The individual accountable for the management, classification, and protection of a specific Information Asset.

PURPOSE:

Establish standardized classification levels for the Division's Information Assets and to define the required level of protection for each classification.

All Information Assets shall be classified based on their sensitivity, legal requirements, and the potential impact of unauthorized access, disclosure, alteration, or loss.

INFORMATION CLASSIFICATION LEVELS

1. Level 1: Public:
   1.1. Definition: Information intended for public access or distribution. Disclosure presents no risk to the Division or individuals.
   1.2. Examples:
      - Information published on the Division or school websites

- Public announcements and newsletters
- Annual reports
- School calendars
- Staff directories containing business contact information

2. Level 2: Internal (Default):
   2.1. Definition: Information used for routine Division operations and everyday work activities. This classification applies to the majority of documents, communications, meetings, and operational materials created or used by Division staff. Information classified as Internal may be shared externally when appropriate for normal Division operations (for example, communication with parents, community partners, or service providers), provided the information does not contain sensitive personal information requiring higher protection. Unauthorized disclosure would typically have minimal impact and would not normally cause significant harm to individuals or the Division.

   2.2. Examples:
   - Lesson plans and classroom materials
   - Student assignments and learning resources
   - Routine communication with parents
   - Internal staff communications
   - Division email communications
   - Internal budgets and planning documents
   - Operational procedures and planning documents
   - Standard meeting invitations and calendar entries
   - Draft curriculum materials

3. Level 3: Confidential
   3.1. Definition: Information containing collections of personal or operational data that should only be accessed by authorized staff members. Unauthorized disclosure could result in privacy risks, operational disruption, or reputational harm and may require notification under applicable privacy legislation.

   3.2. Examples:
   - Spreadsheets containing student information
   - Class lists including student contact details
   - Enrollment reports and demographic data
   - Employee personnel files and employment applications
   - Internal reports containing personal information
   - Contracts and agreements

4. Level 4: Restricted
    4.1. Definition: Highly sensitive information subject to specific legal, contractual, or regulatory safeguards. Unauthorized disclosure could cause severe harm to individuals or the Division and will likely trigger mandatory breach reporting obligations.
    4.2. Examples:
        - Payment card information (card numbers, CVV/CVC codes)
        - Health information linked to an identifiable student or employee, including diagnosis, treatment, or care information
        - Sensitive student support services records (e.g., counselling or psychological records)
        - Information subject to special legal or government security requirements
        - Disciplinary or employee investigations

5. Roles and Responsibilities
    5.1. Authorized Users
    5.2. Authorized Users shall:
        5.2.1. Recognize personal and sensitive data within their work;
        5.2.2. Handle Information Assets in accordance with their classification;
        5.2.3. Take reasonable precautions to prevent unauthorized access, disclosure, or loss.

6. Information Asset Owners
    6.1. Information Asset Owners shall:
        6.1.1. Select or maintain appropriate sensitivity labels when working with Confidential or Restricted information;
        6.1.2. Review and update classifications and associated risk assessments when significant changes occur to the Information Asset, including changes in use, sensitivity, legal requirements, system architecture, or access permissions.
        6.1.3. Ensure compliance with the Division's records retention schedule;
        6.1.4. Confirm that appropriate safeguards are implemented.

7. Information Technology (IT) Services
    7.1. IT Services shall:
        7.1.1. Maintain and support this classification framework;
        7.1.2. Ensure appropriate technical safeguards are implemented based on classification level;
        7.1.3. Maintain an inventory of Information Assets;
        7.1.4. Provide approved encryption tools for authorized off-site transport of Confidential or Restricted information;

7.1.5. Review the effectiveness of this policy periodically, and at minimum every two years, and update it as necessary to reflect changes in legislation, technology, operational practices, or lessons learned from security or privacy incidents.

8. Privacy Officer

8.1. The Privacy Officer shall:

8.1.1. Provide oversight and guidance regarding the protection of personal information in accordance with applicable privacy legislation;

8.1.2. Coordinate the investigation and response to suspected or confirmed privacy breaches involving Division information assets;

8.1.3. Provide advice and recommendations regarding privacy risks and appropriate safeguards;

8.1.4. Recommend updates to policies, procedures, and practices to support compliance with applicable privacy legislation.

REFERENCES

Protection of Privacy Act
Protection of Privacy Act Regulations
Access to Information Act

**Approved:** May 11, 2026