MEDICINE HAT COLLEGE

PROCEDURE

Procedure Name	**DATA STORAGE AND USE** *Revised*		
Procedure Number	**IT 1.2**	Approval Date	May 13, 2026
Parent Policy	IT 1.0 Governance and Access Management		
Procedure Authority	Director, Information Technology		
Executive Sponsor	Vice-President, Administration and Finance		
Approved By	Vice-President, Administration and Finance		

1. PURPOSE

Medicine Hat College (MHC) has established requirements for the secure storage and transport of electronic data. These practices reduce risks related to unauthorized access and data loss, ensuring that data is stored in approved locations, accessed only by authorized individuals, and handled responsibly both on campus and when working remotely.

2. SCOPE

This procedure applies to the access, storage, and transport of all institutional data, regardless of device or location, as well as the users of that data.

3. DEFINITIONS

- **Confidential Data:** non-public, proprietary, or sensitive data shared between parties that is intended to remain private and protected from unauthorized disclosure. Unauthorized disclosure or loss of this data may cause financial and/or reputational damage to MHC and its employees, and/or harm to the individuals to which the data pertains.
- **Institutional Data:** data owned by the college or for which the college is responsible. This includes but is not limited to internal, confidential, restricted, personal, and high-sensitivity data as defined in the Data Classification Standard.
- **Internal Data:** data that is used internally and can be safely circulated between college employees. Unauthorized disclosure or loss of this data may result in inconvenience but is unlikely to cause financial or reputational damage to MHC, or harm to any individual.
- **Personal Device**: an electronic device such as a tablet, cell phone or laptop, purchased by or for an individual, including devices purchased using Professional Development Funds and are not primarily intended for work use.

4. DIRECTIVES

4.1 All college-held information falls within a designated classification category as outlined in the Data Classification Standard. This standard supports the consistent protection of information, appropriate access and legislative compliance.

4.2 Any data with an indeterminate category will be considered confidential data and must be treated as such.

4.3 Electronic data is stored and used in ways that minimize the risk of unauthorized access, loss, or corruption. These practices must comply with privacy policies and applicable data and privacy legislation and should follow industry best practices wherever possible.

4.4 Institutional data must be stored in locations authorized by the college as indicated in the Data Classification Standard.

4.5 Data storage and use requirements apply equally to on-campus, remote, and mobile work environments, protecting the integrity of all MHC data.

4.6 Information Technology Services (ITS) may authorize additional storage locations or methods of use for institutional data when such use supports regulatory compliance, partnership obligations, or enhancements in the productivity and efficiency of college operations.

4.7 To mitigate risk and support accountability, access and use of institutional data is monitored and controlled in alignment with institutional responsibilities.

4.8 Institutional data must be access and used only by those persons who have a legitimate business need.

4.9 Before authorizing any new system or service that uses, stores, or processes institutional data outside the college's on-premises data centre, an Outsourced Risk Assessment (ORA) must be conducted to ensure appropriate safeguards are in place. A Privacy Impact Assessment (PIA) may also be required.

4.10 Internal, confidential, and restricted information may only be viewed or accessed on personal devices through ITS-approved software platforms. This data must not be stored, downloaded, or saved directly to personal devices because they are not managed, monitored, or secured by ITS; therefore, they do not meet the college's security and data-protection requirements.

4.11 Loss or compromise of college managed devices, or personal devices that access college systems and/or institutional data, constitutes a security breach. Such incidents must be reported immediately to ITS and, where applicable, to the Privacy Office.

ORIGINAL COPY SIGNED

_____

Wayne Resch
Vice-President, Administration and Finance
Date: May 13, 2026

Additional Information	Location
Data Classification Standard	MHC Website (internal only)/Policy & Procedure SharePoint

MHC ERM
RISK ID: 4.2 Availability and Continuity; 4.3 Integrity; 4.8 Data, Privacy, and Security