MEDICINE HAT COLLEGE

PROCEDURE

Procedure Name	**ACCEPTABLE USE** *Revised*		
Procedure Number	**IT 1.1**	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) is committed to promoting the responsible and effective use of its information technology (IT) resources. These resources are provided to support the college's academic, administrative, and operational functions and must be used in a manner that is ethical, responsible, and secure. The following acceptable use expectations protect institutional data, maintain system integrity, and help sustain a secure and productive environment.

2. DEFINITIONS

- **Authentication Account:** a unique digital identity, like an e-mail or login account, that is assigned to an individual, system, or service. Authentication Accounts are used to verify and authorize access to college IT Resources.
- **Information Technology Resource (IT Resource):** any hardware, software, digital service, account, or computing system owned or managed by the college that creates, stores, processes, transmits institutional data, or connects to a college network. If you are unsure if something is an IT Resource, contact ITS.
- **Least Permissive Principle:** a security and access control principle that ensures users, systems, or processes are granted the minimum level of access or privileges necessary to perform their required tasks.

3. DIRECTIVES

3.1 Those who use IT resources are responsible and accountable for their actions and communications in the college environment and use these resources in an ethical, responsible, and secure manner that complies with all applicable laws, regulations, licensing agreements, policies, procedures and standards.

3.2 Users are provided with authentication accounts to support their official roles and responsibilities. All authentication accounts will use the Least Permissive Principle. This approach reduces the risk of unauthorized actions or potential security breaches by limiting exposure. Users are responsible for taking precautions to prevent unauthorized access to these accounts and all IT resources allocated to them. These authentication accounts must not be shared without written approval from IT Services.

3.3 To help safeguard the security of college systems, data, and users, access to authentication accounts and IT resources may, when necessary, be suspended or restricted without notice. This may also occur if an account appears to be in violation of applicable laws, regulations, licensing agreements, policies, procedures, or standards. Affected users will be provided with

information on the reason for the action and guidance on the steps required to restore access as quickly as possible.

3.4 All official college business must be conducted through MHC managed communication systems unless authorized by ITS to ensure IT security, institutional data protection, and compliance with Alberta privacy legislation. Users should check their MHC email accounts regularly for timely updates. However, the college retains the right to contact employees via personal communication methods when necessary for business purposes.

3.5 While IT resources and services are provided for work-related activities, limited personal use is permitted, provided it does not result in a conflict of interest, interfere with work responsibilities, consume significant resources, or violate MHC policies, procedures, and standards.

3.6 MHC accounts must not be used to facilitate the provisioning of services not related to the college. For example, employees cannot use their authentication account to sign up for newsletters or websites based solely on personal interest.

3.7 Upon enrolment students are provided with authentication accounts and applicable IT resources to support their academic activities. Access to these services is maintained while students are actively attending the college but will be suspended when they are no longer considered active.

3.8 Responsible use of IT resources protects the college from exposure to security, privacy, reputational, and litigation risks. Unacceptable use may result in disciplinary action.

ORIGINAL COPY SIGNED

_____

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

MHC ERM

RISK ID: 4.8 Data, Privacy, and Security; 4.3 Integrity