Medicine Hat College Policy
MOBILE IT CONNECTIVITY

Policy #:	IT-01
Policy Authority:	Director, Information Technology
Executive Sponsor:	Vice-President, Administration and Finance
Approved by:	President and CEO
Effective Date:	May 4, 2022
Next Mandatory Review Date:	May 4, 2025
Frequency of Review:	Every 3 years

1. OBJECTIVE

This policy facilitates connection to, or remote access of, ITS networks, infrastructure, systems, and information (data) using mobile computing and communication devices, or through remote access, as outlined in this policy.

2. SCOPE

This policy applies to all employees requiring access to college systems, services, and information through mobile computing and communication devices (college or approved personal devices.)

3. DEFINITIONS

- **Access:** the ability to access a Medicine Hat College (MHC) owned or controlled computer, an MHC owned or controlled network, or a cloud system/service.
- **College Allocated Mobile Device:** a device provided to employees with specific job roles as indicated in Appendix A – Eligibility for a College Purchased Mobile Device and Data Agreement.
- **Microsoft 365:** includes Microsoft Office applications, Microsoft Exchange email and calendar tool, Microsoft OneDrive, and Microsoft Teams used by MHC for all employees and authorized users.
- **Mobile Device:** includes computers, laptops, cell phones, smartphones, PDAs, and tablet devices that synchronize with or remotely access college owned or supplied services, networks, or computer systems.
- **Mobile Internet Connectivity:** refers to Wi-Fi or cellular provided internet connectivity through a pay for service agreement with an internet service provider.
- **Multi Factor Authentication (MFA):** an electronic authentication method in which a user is granted access to a website, application, or a device after successfully presenting two or more pieces of evidence to an authentication mechanism, for example, the use of both a password and authentication approval through an authenticator application.
- **Personal Device:** a mobile device owned by the individual, not by the college.

- **Single Factor Authentication (SFA):** a method of securing access to a device, system, or resource that identifies the party requesting access through only one category of credentials, for example, a password, or PIN.

4. PRINCIPLES

MHC relies on information technology resources to conduct its business and is committed to ensuring the integrity and security of data by enacting protections and controlling user access.

5. DIRECTIVES

5.1 All users that synchronize with or use remote access to access college owned or controlled physical, virtual, and cloud IT network infrastructure and systems, including email, scheduling, or calendaring systems, must be authorized to do so.

5.2 Access will be controlled, not all employees will be able or authorized to access, nor will all resources be made available.

5.3 MHC will put in place user, network, and device access controls and user and device security measures as it sees fit to protect college IT infrastructure, networks, data, and to secure data integrity, security, and privacy.

5.4 MHC will determine which employees require a college allocated mobile device for their job role as indicated in Appendix A – Eligibility for A College Purchased Mobile Device and Data Agreement.

5.5 Negligent use or abuse may result in revocation of connectivity privileges and the individual reimbursing the college for any costs incurred by the college.

5.6 Users issued with a college owned device for work purposes will not be eligible to request to use their own personal device for work until the college owned device is up for renewal.

5.7 Information Technology Services (ITS) approves what devices are supported and purchased by the college.

5.8 ITS is responsible for the approval and purchasing of college supported devices.

5.9 Eligibility and Conditions of Use for Personal Devices

5.9.1 MHC employees and authorized non-employees may synchronize devices to MHC's Exchange email and Calendar system, and Microsoft Teams application. Personal owned devices are not allowed to synchronize with MHC Microsoft OneDrive.

5.9.2 Employees who choose to connect a personal device to MHC owned or controlled systems do so entirely at their own cost and risk.

5.9.3 Shared accounts (college accounts accessed by more than one person) will not be synched to personal devices.

5.9.4 Users who choose to sync their personal device with the college's MS Exchange or other college owned information systems or services accept that there may be some inadvertent risk to personal information.

5.9.5 Any security application or feature required on the device is the exclusive responsibility of the device owner.

5.9.6 MHC cannot guarantee connectivity, service quality, and technical or use support of personal devices. However, IT Services will attempt to assist with the configuration and use, or direct users to assistance, as able and practical for MHC.

5.9.7 MHC is not responsible for personally owned equipment, including damage, configuration,or data loss relating to its use or configuration for use on any MHC system.

5.10 Lost, Stolen, or Compromised Devices

Owners of devices provided by the college or personal devices that access or synchronize with MHC systems must immediately report to their supervisor and ITS:

(a) if the device is lost, stolen, compromised, or is suspected to have been compromised.

(b) any incident or suspected incidents of unauthorized data access, data loss or disclosure of MHC information resources, databases, networks, etc.

5.11 Security Requirements for Devices that Synchronize to Microsoft 365

5.11.1 Devices that synchronize with MS Exchange, MS Teams, and MS OneDrive must be encrypted.

5.11.2 To access the device, a password, PIN, or biometric authentications must be used. (Single Factor Authentication.)

5.11.3 The PIN or password must be at least four characters that are not trivial (not a series of repeated characters like 1111 or a sequence of numbers like 1234.)

5.11.4 The device must enter an inactivity timeout (lock) and require a minimum of a single factor authentication after no more than thirty minutes of inactivity.

5.11.5 If determined by MHC, the device must have MHC authorization security or authentication installed (Multi Factor Authentication.)

6. RESPONSIBILITIES

Director, Information Technology is responsible for approving access of mobile devices to MHC's IT infrastructure, electronic data stores and services, and college owned IT equipment.

7. RELATED POLICIES

5.19 Information Technology Acceptable Use Policy
8.12 Allocation of Microcomputers

8. RELATED PROCEDURES

PR-IT-01-01

9. RELATED INFORMATION

Appendix A – Eligibility for a College Purchased Mobile Device and Data Agreement

ORIGINAL COPY SIGNED

Kevin Shufflebotham
President and CEO

Date: May 4, 2022

ORIGINAL COPY SIGNED

Wayne Resch
Vice-President, Administration and Finance

Date: May 4, 2022

DOCUMENT HISTORY

April 2016	Policy approved
May 2022	Revised policy approved