Information Technology Acceptable Use Policy

Responsibility	Director of IT	**Review Period**	5 years
Approving Body	President's Council Senate	**Initial Approval Date**	August 22, 2017
Advisory Body	IT Committee	**Latest Approval Date**	March 22, 2017 (Pres Co) August 22, 2017 (Senate)
Status	Approved	**Next Review Due Date**	August 22, 2022

Purpose and Scope

This policy describes the acceptable use of Information Technology (IT) Resources in support of the mission of Canadian Mennonite University (CMU). It builds on the principles of accountability, transparency, privacy, and fairness to support a functional environment for work and study in which these resources are protected. This policy applies to anyone who uses or accesses any IT Resource belonging to, under the control or in the custody of, Canadian Mennonite University.

CMU provides IT Resources to support the teaching, learning, research, service, administrative, and community development and business activities. As valuable assets, they need to be used and managed responsibly to ensure their integrity, security, and availability for the stated purposes.

This policy is intended to outline the acceptable use of CMU IT Resources and to protect the Authorized User and CMU. Inappropriate use exposes CMU to risks including virus and spyware attacks, breaches of network systems and services, criminal charges in the case of a violation of legislation, or litigation should the terms of a contract be contravened. This policy is not intended to impose restrictions that are contrary to CMU's established culture of openness, trust, integrity, and academic freedom.

It is the responsibility of every authorized user to know these guidelines, and to conduct their activities accordingly.

The IT Administrators shall be responsible for the development, administration, and maintenance of procedures to be implemented in compliance with this policy.

Definitions

"Account" includes any username, access code, password, PIN, credential, or other form of authentication, which has been assigned to Authorized Users to use any University IT Resource.

"Admin network" refers to the network on which only University-owned devices are allowed, and accessible only by University employees. This network allows access to University resources which are limited to University employee access. It is accessible throughout the administration and classroom areas on campus. The wireless name (SSID) is CMUAdmin and the key is not to be shared with those not authorized to connect to the Admin Network.

"Authorized" means specific access rights granted in accordance with University governance or policies.

"Authorized user" means an individual who is an employee, student, alumni, associate, or other individual who has been granted access to use any University IT Resource.

"IT Administrator" means an individual responsible and authorized to establish or maintain and provide technical support for a University IT Resource, and responsible for monitoring compliance with the Acceptable Use Policy.

"Information Technology (IT) Resource" means any information, data, software, hardware, system, or network belonging to, under the control or in the custody of the University, regardless of who administers it.

"Personal Information" means recorded information about an identifiable individual, and as defined in federal and provincial privacy legislation.

"Residence Network" refers to the network accessible in the residence buildings for resident and guest use. It provides connectivity to the internet through the University firewall, but does not allow access to other University IT Resources such as printers or servers.

Acceptable Use

Personal Use

CMU permits limited personal use of CMU IT Resources on the Admin Network, and unlimited personal use of CMU IT Resources on the Residence Network and external networks. Personal use must not violate any law, statute, or CMU policy. Users who require a private means of computing or sending electronic communications should utilize a personal device unconnected to the University's IT network.

The CMU Residence Network is supplied by CMU for the personal use of residence students and guests. The provisions of this policy apply to the use of the Residence Network, and additional guidance for students is provided in the Student Handbook.

Privacy

CMU respects the privacy of all users of its IT Resources, and uses reasonable efforts to maintain confidentiality of Personal Information. All network traffic must go through CMU's firewall, where it is filtered and logged. Circumstances may arise in which such privacy cannot be maintained. Such circumstances include, but are not limited to, the following:

- Access to Personal Information may be granted by the appropriate Vice President (or designate) to an Authorized User, System Administrator, or agent to meet legitimate CMU business needs and operational requirements.
- CMU may audit, access, or restore any IT Resource within its environment when it has reasonable grounds to suspect a breach of acceptable use or a possible violation of any law or University policy.

For security and network maintenance purposes, authorized individuals at CMU may monitor equipment, systems, and network traffic at any time.

Good Judgment

Authorized Users must exercise good judgment in determining what is acceptable use of IT Resources with due regard to this policy, other University policies, and the ethos of the University community. Some activities may

be appropriate in a specific context (e.g. for authorized academic and research purposes), while some are not appropriate in any context. The University firewall provides a level of malware protection on both the Admin and Residence Networks, and also provides a landing page to warn of material that could potentially violate University policies.

Authorized Users have an obligation to take all reasonable steps (e.g. password protection and strengthening) to protect the confidentiality, integrity, and availability of IT Resources and report encountered vulnerabilities to an IT Administrator. Failure to do so may constitute a breach of this policy.

Examples of a Breach of Acceptable Use

Unless explicitly authorized, a breach of acceptable use includes, but is not limited to:

1. Allowing others to access your assigned personal Accounts.
2. Failure to exercise reasonable care in safeguarding Accounts and information.
3. Accessing someone else's personal Accounts.
4. Seeking information on passwords or information belonging to others.
5. Breaking or attempting to circumvent licensing or copyright provisions.
6. Copying, deleting, intercepting, or examining someone else's files, programs, or information.
7. Attempting to collect, use, or disclose, the Personal Information of others.
8. Using IT Resources to harass or bully others.
9. Attempting to circumvent information security provisions or exploit vulnerabilities.
10. Effecting security breaches or disruptions in network communication, including, but not limited to: network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning and executing any form of network monitoring which will intercept data not intended for the user's host.
12. Using IT Resources (e.g. CMU Network Account or workstation) for unauthorized commercial purposes.
13. Any interference with the ability of others to use IT Resources whether it is disruptive or not.
14. Falsifying or misrepresenting your identity for malicious purposes.
15. Using IT Resources to actively engage in procuring, transmitting, storing, or viewing pornographic or offensive material.
16. Distributing or disseminating pornographic or offensive material in any location.
17. Installation of unlicensed software on University IT Resources.

Outcomes and Enforcement

Authorized Users must be aware that their network traffic can be monitored without prior notice.

If the integrity or security of an IT Resource is compromised or at risk, an IT Administrator may authorize the locking or quarantining of an Account or resource at his or her sole discretion. Upon reasonable belief by an IT Administrator that a violation of this policy has occurred, an investigation will be undertaken by an IT Administrator.

If access to any Personal Information is required, authorization from the appropriate Vice-President (or designate) will be requested.

If a violation is determined to have occurred, the following actions may be initiated by the investigating IT Administrator:

Class or severity	**Possible outcomes**
Minor violation of the AUP	Warning
Serious or repeated violation of the AUP	Escalation to appropriate authority or disciplinary process and/or restrictions on access or use
Possible violation of federal, provincial, or municipal law or statute.	Forward for investigation to other relevant authorities

Related Policies

This Acceptable Use Policy prohibits any use of IT Resources which violates any other CMU policy, code, or agreement, constitutes academic or non-academic misconduct, or which violates federal, provincial, or municipal laws or regulations.

In addition to outcomes under the AUP, such violations may be prosecuted under those laws and policies. Any information resulting from an investigation under the AUP may be shared for the purposes of such prosecutions.

[End of document]