Part 10 - Information Technology Services
Acceptable Use of Computing and
Communication Resources Policy
POL 1050

Policy Type:	Management		
Policy Sponsor:	Vice-President, Administrative Services	**Effective:**	February 20, 2014
Office of Administrative Responsibility:	Chief Information Officer, Information Technology Services	**Last Reviewed:**	February 2014
Approver:	Board of Governors	**Approved:**	February 10, 2014

A.   OVERVIEW

As a part of the physical and social learning infrastructure, Mount Royal University acquires, develops, and maintains its own computers, computer systems, and networks. These computing resources are intended for institutional-related purposes, including direct and indirect support of Mount Royal University's instruction, research, service missions, and administrative functions. These computing resources are also intended for student and campus life activities and the free exchange of ideas among members of the Mount Royal community and wider local, national, and world communities.

The use of Mount Royal computing resources, like the use of any other institution-provided resource and any other institutional-related activity, is subject to compliance with legal and ethical behavior within the Mount Royal community.

Mount Royal's Information Technology Services Department is available to assist, advise and consult with users on the proper use of institutional computer resources and interpretation of the Policy. If there are any questions or uncertainty about the Policy, users are encouraged to contact the Chief Information Officer or their designate for clarification.

This Policy should be read in conjunction with the following policies: *Policy 845-1 Employees Safe Disclosure of Wrongdoing and Public Interest Disclosure Policy, Policy 845-2 Safe Disclosure Policy - Non Employees, Policy 513 Code of Student Conduct, Policy 1704 Personal Harassment Policy, Policy 1702 Human Rights Policy,* and *Policy*

1073 Offensive/Discriminatory Material as well as all other Mount Royal University policies.

B.   PURPOSE

This Policy outlines the general usage policy all users of Mount Royal University computer and communication resources must abide by. Mount Royal computing and communication resources are provided for "institutional-related purposes."

Recognizing, however, it may be difficult to distinguish between personal use and "institutional-related" uses, the costs associated with occasional personal use, the costs associated with enforcing a flat prohibition, and the benefits that may accrue to Mount Royal from increased experience and familiarity of its users with available computing resources, "incidental" personal use is permitted only to the extent that there is compliance with University standards as well as federal, provincial and municipal law and regulations.

C.   SCOPE

This Policy applies to all users of Mount Royal University owned or licensed computing resources, whether on campus or from remote locations. Additional policies may apply to specific computers, computer systems, or networks provided or operated by specific units of Mount Royal.

Mount Royal computer and communication resources are defined to include but are not limited to such devices as desktop computers, laptop/tablet computers, monitors, hard drives, disk space, printers, scanners, network devices, data capable phones (smartphones), internet access and networks provided by the University, including computer labs, and software acquired by Mount Royal. This Policy is also extended to include any computer system or resource that is owned or managed by Mount Royal University regardless of its location.

D.   POLICY STATEMENT

All users of Mount Royal University computing resources must:

(1)   Comply with all federal, provincial, and other applicable statutes; all applicable Mount Royal policies and procedures; and all applicable contracts and licenses. Such laws, rules, policies and procedures, contracts, and licenses include, but are not limited to, the laws of defamation, privacy, copyright, trademark, obscenity, Mount Royal's *Code of Student Conduct, Human Rights Policy* and *Personal Harassment Policy* as well as the *Criminal Code of Canada* which prohibits "hacking," "cracking," and similar activities. Users who engage in electronic communications with persons in other provinces or countries or on other systems or networks should be aware that they may also be subject to the laws of those other provinces and countries and the policies and procedures of those other networks. Users are fully responsible for ascertaining, understanding, and complying with the laws, rules, policies and procedures, contracts and licenses applicable to their particular uses.

(2)   Use only those computing resources that they are authorized to use and they may use them only in the manner and to the extent authorized. The technical ability to access computing resources does not necessarily mean there is authorization to do so. Users are responsible for ascertaining the necessary authorizations and to obtain them before proceeding.

(3)   Only consume the amount of resources required to perform an authorized task at Mount Royal University. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of Mount Royal computing resources, Mount Royal may require users of those resources to limit or refrain from specific uses in accordance with this principle or other policies and procedures outlined by Mount Royal. Users are also required to use printing, scanning and copying resources responsibly. Users are expected to manage file storage based on University Records Retention Policy and their needs.

(4)   Be aware that their use of Mount Royal University computing resources is not completely private. While Mount Royal does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of Mount Royal resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, the scanning of systems and network ports for anomalies and vulnerability, and other activities that are necessary for the rendition of services.

(5)   Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Having the ability to access other person(s) accounts does not necessarily mean there is authorization to do so. Users are responsible for ascertaining the necessary authorizations and to obtain them before proceeding. Respect the privacy of others by not tampering with their passwords, accounts or files, or by representing others when messaging, conferencing or accessing electronic resources. Respect the rights of others by complying with all University policies regarding sexual, racial and other forms of harassment and by preserving the privacy of personal data to which you have access.

(6)   Using MRU computing resources for user's commercial purposes - for personal financial or other gain is not allowed and, under some circumstances, may be illegal.

(7)   Note that materials not subject to legal sanction may be objectionable or extremely offensive to persons other than the computer user. Importation or distribution of such material (including, but not limited to racist material, hate literature, sexist slurs or sexually explicit material) is permitted for academic or research purposes as long as it complies with Mount Royal's Offensive/Discriminatory Materials Policy. In some cases, it is recommended that prior consultation with a Faculty Member, Chair or Dean be obtained to ensure that Mount Royal's community and ethical standards are maintained. Consultation with the Information Technology Services Department or University Library is available in order to facilitate those activities.

(8)   Note that users are not permitted to remove or disable any security software installed by IT Services from workstations connected to the Mount Royal network.

This includes, but not limited to, anti-virus software, workstation management software, and agent components thereof.

(9)   Note that all software installed on Mount Royal University-owned systems must be properly licensed to Mount Royal. Users are typically not permitted to install software on any Mount Royal-owned device unless specifically authorized to do so. Users are encouraged to work with Information Technology Services on the acquisition and installation of any software required to do their work for Mount Royal.

(10)   Keep in mind that users of Mount Royal computing and network resources are responsible and accountable for their actions and statements in the electronic working and learning environment.

(11)   Make every effort to prevent the unauthorized disclosure and distribution of information that is the property of Mount Royal University.

(12)   Users must not intentionally introduce viruses into Mount Royal computer systems.

(13)   Abide by specific Student Guidelines (see Appendix A) if attending Mount Royal University as a student either part time or full time.

(14)   Note that users of Mount Royal University-owned devices used at home must still abide by this Policy statement as well as other Mount Royal policies including, but not limited to, Policy 1025 Internet and Network Access at Mount Royal University.

E.   DISCIPLINE, JURISDICTION AND PENALTIES

If Mount Royal University learns that there is an inappropriate use of Mount Royal computing resources that conflicts with this outlined Policy, Mount Royal may take disciplinary action. The Information Technology Services Department will investigate properly identified allegations/suspicions to ensure compliance with applicable, federal and provincial laws and with institutional policies and procedures and report all such incidents by employees to the Associate Vice-President, Human Resources or such incidents by students to the Office of Student Conduct.

RELATED LINKS

(1)   Policy 1050 Appendix A: Student Lab Guidelines

POLICY 1050
Appendix A

STUDENT LAB GUIDELINES

The following protocols, rules and regulations are implemented as the result of a request that students have equal and secured access to the computing equipment, software programs, accessories and working space:

(1)   At the start of each session on a computer, students must log on properly and subsequently log off. The computer equipment will be treated with respect; any accident and/or damage must be reported to the lab monitor or Information Technology Services Department immediately to ensure additional damage does not occur.   Students may be held accountable for the repair or replacement costs for damaged or lost equipment.

(2)   Absolutely no food of any type will be allowed in the computer labs unless it is secured in a storage receptacle (i.e. backpack). All drinks must be contained in cups with attached lids.   Getting food and spills from drinks onto keyboards and computers causes expensive damage to the equipment. Students may be held accountable for the repair or replacement costs for damaged equipment.

(3)   Only registered students, authorized users, faculty or Mount Royal employees are permitted in the computer labs to use Mount Royal computer resources. Public/guests are permitted to use the equipment identified for their use in designated locations.

(4)   Any student, who breaches the security system in any manner, including lending their access security card to others, may have their privilege to use Mount Royal's computer resources revoked.

(5)   Students may leave a computer on and unattended for no more than 15 minutes. If a computer is left on unattended for more than this allotted time, other would be entitled to take over use of the computer. This could result in the loss of in-progress work.

(6)   The computer may be shut down if unattended for more than 15 minutes by faculty, staff or designated computer lab monitors.

(7)   It is the responsibility of each user to ensure that all transitory storage media such as USB flash drives, CDs or DVDs are free of any and all viruses before they are used with Mount Royal computer systems.

(8)   Students will be liable for any and all intentional damage caused to the computer systems, networks, and/or data. Students are encouraged to always practice safe computing and make sure they have a back up of all their important data files at all times.