INFORMATION TECHNOLOGY (Computer Technology)
ACCEPTABLE USE

Section:	General Administration
No:	5.19
Effective Date:	October 2002
Revised:	March 2009
Approved by:	President

Background – Authority and Scope

Access to the computing and network environment at MHC is to be used in effective, ethical and lawful ways that support the values of the college. This agreement stipulates the rights and responsibility of users of this equipment. Medicine Hat College (MHC) provides faculty and staff with computer equipment and related technology to enable them to perform their jobs.

All people (employees, students, or otherwise) accessing or otherwise using information technology resources owned and /or controlled by Medicine Hat College are bound by the stipulations of this agreement.

Note that MHC is the owner of this equipment and is thereby responsible for its appropriate use. MHC has the right to limit or deny use of equipment if it is being used for inappropriate activity, either as stipulated in this agreement or based on legislation of Canada or Alberta.

Authority

The Board of Governors of Medicine Hat College has authority over this policy. Administration of this policy and the associated procedures are delegated to the college's senior executive officers.

Application

This policy and related procedures applies to all individuals employed by the college, all students of the college and all visitors and community users who use the college's computer resources and services.

This college-wide policy applies to the use of computers, data networks and the resources these technologies make available in support of the college's activities. It applies to any devices and/or computers owned by the college, as well as those owned by users who have been authorized to install or connect personal equipment either on the premises or to the network.

College computer 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, personal digital assistant devices (PDAs), cellular phones, smart phones, network routers, network bridges, network switches, servers, access to the Internet and other networks provided by the college including wireless, computer labs, software acquired by the college and relevant data. This section includes any computer system or resource that is owned or managed by the college regardless of its location.

Principles

The following principles are the basis of managing the college's computer resources in an ethical and effective manner.

1. The college will maintain an atmosphere that balances respect for individual computer usage and college computing needs.

2. The college will maintain an environment whereby the college's computer resources are considered to be reliable, secure and efficient.

3. All college computer resources shall be used primarily for work-related activities (i.e. educational, academic research, and administration purposes) and as such using the college's computer resources and access to the Internet for incidental personal purposes shall be minimized.

End User Rights and Responsibilities

MHC employees have the right:

1) To be provided with an appropriate level of computer technology (software and hardware) to allow them to perform their jobs.
2) To have the computer technology maintained and repaired in a timely manner.
3) To load work-related software on their MHC provided computer system, as long as the software is proven to be legally licensed, does not pose a reliability or security risk, and is related to their work at MHC.

MHC has the right:

1) To deny use of MHC computer equipment or related services based on the contents of this policy, or if the college executive regards the use to be inappropriate or to pose risk to the college.
2) To monitor use of MHC computer equipment and related infrastructure based on Guideline 4 below.

Guidelines for the Use of College Computing Resources

1. Individuals using college-owned computer resources are expected to comply with provincial and federal laws and relevant MHC policies and procedures. Users should note that some of the material used at the college is copyrighted, protected by intellectual property law and/or license agreements. Users must ensure that they do not violate the various laws, policies, procedures and license agreements.

2. Users of college computing and network resources are responsible and accountable for their actions and statements in the electronic working and learning environment.

3. Users are expected to use reasonable restraint in consumption of these valuable shared resources, and to use them in ways that do not interfere with the study, work or working environment of other users.

4. Any data stored or transmitted using MHC technology may be monitored by the college. Such data will not be accessed by the college without cause and due process.

5. In any circumstances of alleged or suspected impropriety, the college will examine directories, files, email or other electronic records that are relevant to the investigation.

6. Users accessing external networks such as accessing the Internet or SuperNet through college computing and network resources are bound by both external policies and the college's policies. Users should be aware that the more restrictive of the policies will apply.

7. Anyone who observes actual or apparent use by employees which appears to violate this policy or other Information Technology Services policies will report it to the Director, Information Technology.

8. Anyone who observes actual or apparent use by students or public visitors which appears to violate this policy or other Information Technology policies will report it to

the appropriate authority which may include Director, Information Technology so that appropriate action may be considered.

Support

Medicine Hat College's Information Technology Services is available to assist, advise and consult with users on the proper use of college computer resources and interpretation of this policy. If there are any questions or uncertainty about this policy, users are encouraged to contact the Director, Information Technology.

Unacceptable Uses

Below are a number of examples of unacceptable uses of college computing resources. The list is not comprehensive but serves to guide users of the types of activities that are not permitted.

1. Unauthorized access (e.g. hacking, phishing or pharming): this may include using unauthorized user names, passwords, computer addresses or identities or modifying assigned network settings to gain access to computer resources and/or data, or otherwise attempting to evade, disable or crack security provisions of college or external systems. The Criminal Code of Canada has two related sections: Section 342.1 - Unauthorized use of computer and Section 342.2 - Possession of device to obtain computer service. (http://www.canlii.org)

2. Unauthorized Distribution and Disclosure of Information: every effort must be made to prevent the unauthorized disclosure and distribution of information that is the property of MHC.

3. Vandalism or Destruction of data: deliberate alteration or destruction of computer files is a Criminal Code offence (Section 430.1). Under no circumstance may a user inspect, alter, delete, publish or otherwise tamper with files or file structures that the individual is not authorized to access. The Freedom of Information and Protection of Privacy Act (FOIP) also deals with deliberate destruction of data.

4. Deliberate interference with other users' work: this includes use of any process that causes other users to be deprived of services or resources that they would normally expect to have available. It covers but is not limited to the creation of spam (excessive email distribution), downloading or electronic transferring of excessively large resources and/or the deliberate introduction of viruses or electronic chain letters.

5. Sharing of accounts: the college's computing resources are allocated to groups and individuals for specific educational, academic research and administrative purposes.

It is not acceptable to give, sell, or otherwise provide computing resources to other individuals or groups that do not have explicit permission to use them. Users are not to share computer accounts without getting permission from the college administration or Information Technology Services.

6. Commercial uses: use of the college's computer resources for non-college related commercial use is not permitted.

7. Squandering resources: resources are shared and no user may deliberately degrade the college's computer resources by: unwarranted data space, time and bandwidth consumption through resource-intensive programs, excessively large downloads, excessively large electronic transfer of files, unattended network connections and/or lengthy print jobs. As the use of college resources changes and the technology capabilities change over time – users are encouraged to work with Information Technology Services in defining appropriate and efficient uses of computer resources. In the interest of providing technology enabled services to the college community as a whole, the college reserves the right to terminate access privileges to one or more individuals whose activities when using college computer resources severely impacts services to others.

8. Personal Uses: the college's computer resources are to be used primarily for college purposes (i.e., educational, academic research and administrative). All users have the responsibility to ensure that incidental personal use of college computer resources is minimized and does not interfere with the normal course of their work. Use of a college computer for activities which may bring viruses or spy ware into the computer or the college network is not permitted. Examples of websites which may attract viruses and spy ware are on-line gaming sites, gambling sites and pornographic sites. College computer resources are not provided for the playing of games, viewing pornography, illegal file sharing, or for commercial purposes (i.e., operating a business).

9. Remote Access: remote access of Medicine Hat College's information technology systems is permissible so long as the usage does not compromise or violate either the network, computer, or data security and the ethical principles of the college.

10. Breach of copyright: this includes installing, reproducing and/or distributing copyrighted materials such as proprietary software, publications or files without permission. College software is provided under license agreements with various vendors and may not be copied or otherwise removed. Third party copyrighted information or software that the users do not have specific approval to store and/or use, must not be stored on college systems or networks.

11. Offensive material: materials not subject to legal sanction may be objectionable or extremely offensive to persons other than the computer user (including, but not limited to racist material, hate literature, sexist slurs or sexually explicit material). Importation or distribution of such material may be permitted for academic or research purposes. It is recommended that prior consultation with an instructor, dean or director of a department occurs. If required, consultation with Information Technology Services is available in order to facilitate these activities.

12. Hostile atmosphere: the display of sexually explicit or violent images in public spaces and/or the initiation of unsolicited communication with sexual content may be objectionable or extremely offensive to people. In cases where a presentation requires the display of potentially disturbing material, prior consultation with the appropriate dean or director of a department must occur. If required, consultation with Information Technology Services is available in order to facilitate these activities.

13. Harassment: harassing or defamatory material may not be sent by electronic means, including email and voice mail, or postings to news groups. The Criminal Code of Canada outlines the offense and punishments for Criminal Harassment in Section 264(1) C.C. (http://www.canlii.org)

14. Security Software: users are not permitted to remove or disable any security software installed by Information Technology Services from workstations connected to the MHC network. This includes, (but is not limited to), anti-virus software, workstation management software, and agent components thereof.

15. Software Installation: all software installed on college owned computers, including laptops, must be properly licensed to the college. Users are typically not permitted to install software on any college owned computer. Exceptions to this rule can be made for those users who clearly understand the implications of installing software on college owned computers. These users will be required to sign an agreement outlining their responsibilities. Users are encouraged to work with the Information Technology Services on the installation of any software required to do their work for the college. (Each installation of unlicensed software on college computers which has not been properly licensed to the college could result in a substantial fine by the Canadian Alliance Against Software Theft (CAAST)).

16. Off Campus Computer Use: users of college owned computers which are used at home, or while travelling, or otherwise, must still abide by this policy. Proper and safe computing practices are expected. Users are responsible for the use, content and maintenance of this equipment and software. Any software which is the property of the college must be properly licensed to either the college or to the user.

Discipline, Jurisdiction and Penalties

If the college learns of an inappropriate use of information technology resources, the college may take disciplinary action. Information Technology Services will investigate identified allegations to ensure compliance with applicable federal and provincial laws and with college policies and procedures. All such incidents will be reported to the Director, Information Technology.

a) Employees including contract employees and 3rd party consultants

Human Resources will work with Information Technology Services to determine the extent and nature of the misuse and then Human Resources will work with the individual's supervisor to determine the appropriate level of disciplinary action, which may include termination. Any perceived violations of the law will be reported to the appropriate law enforcement authorities. Any employee discipline will occur in a manner that is consistent with the appropriate collective agreement and policy for employees.

Access privileges may be revoked immediately and long term outcomes may include temporary or permanent loss of access privileges dependent upon the nature and extent of the misuse.

b) Students

The Director of Student Services will work with Information Technology Services to determine the extent and nature of the misuse to determine the appropriate level of disciplinary action. Any perceived violations of the law will result in immediate loss of privileges and will be reported to the appropriate college executives and law enforcement authorities. Lesser violations by students will be dealt with under the academic regulations and policy sections of the Medicine Hat College academic calendar, specifically the "Student Nonacademic Misconduct" and "Social Guidelines" sections.

c) Community Users

A member of the college executive will work with Information Technology Services to determine the extent and nature of the misuse to determine the appropriate level of action. Any perceived violations of the law will result in immediate loss of privileges and will be reported to the appropriate law enforcement authorities. Failure to comply with these guidelines can result in a community user losing their access and privileges to using college computer resources and may include expulsion from the college.