BLUE MOUNTAIN COLLEGE

POLICIES AND PROCEDURES

AREA: **Academic Affairs**

NUMBER: **Policy 2.22**

SUBJECT: **Acceptable Use of Technology**

1. **Overview**

Blue Mountain College online systems are properties of the College that are provided to be used for general business and education purposes to increase production of faculty, staff, and students. To ensure the use of online systems in a productive manner, the institution requires that policies, procedures, and guidelines regarding computer use be strictly adhered to by users. All faculty, staff, and students are required to abide by these policies; any improper use of online systems is not acceptable and may result in disciplinary action, up to and including expulsion and/or termination of employment.

Acceptable use begins with individual responsibility in adhering to all local, state, and national laws. Furthermore, in keeping with the College's mission and goals, all computing use should promote the academic, social, spiritual, and moral development of the campus.

Members of the College community are encouraged to make use of the campus computing system. The campus computing system consists of two parts:

- the Administrative Network which has the purpose of facilitating internal communication and internet resources among all members of the administration; and

- the Student/Public Network which has the purpose of providing Internet resources to all students.

2. **Internet/Network/Social Media Usage**

Access to the Internet and other network resources is provided for Blue Mountain College purposes and must not be abused for personal use. The College's Internet connection provides access to external informational resources via e-mail, FTP, and the World-Wide Web (www). The College maintains a Web page at http://www.bmc.edu through which interested parties may obtain information about the College.

While the College regrets any inadvertent actions that result in the loss of or damage to information, the responsibility for prevention and the resolution of such problems rests with the user. Furthermore, the College will not be responsible for any unauthorized charges or fees resulting from access to the computer system.

Users are expected to act ethically and responsibly in their use and time usage of the Internet/Network/Social Media and to comply with the relevant national legislation, regulations

and codes of practice. Users must not post messages on newsgroups or chat areas that are likely to be considered abusive, offensive or inflammatory by others.
Discrimination, victimization or harassment on the grounds of gender, marital status, family status, religious belief, age, disability, race, color, nationality, ethnic or national origin is against College Policy. Users must not bully, hassle or harass other individuals via Internet/Network/Social Media. Users must not send messages that are likely to be considered abusive, offensive or inflammatory by the recipient(s).

Misuse and time abuse of Internet/Network/Social Media may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, dismissal. The College also reserves the right to report any illegal activities to the appropriate authorities.

All security incidents involving Internet access should be reported to the Blue Mountain College Director of Information Technology Services.

All users must adhere to the following when using College facilities to connect to the Internet:

- Commercial use, which is not connected to or approved by the College, is strictly prohibited and will result in disciplinary procedures.
- Users must not use the College Internet connection to scan or attack other individuals/devices/organizations. The use of port scanners or other hacking tools unless used as part of an approved course of study is strictly prohibited.
- Users should be aware that the public nature of the Internet dictates that the confidentiality and integrity of information cannot normally be relied upon.
- Where a requirement exists to send or receive confidential or commercially sensitive data over the Internet, a security mechanism recommended by the Director of Information Technology Services should be used.
- Software copyrights and license conditions must be observed. Only licensed files or software may be downloaded from the Internet.
- The use of the College Internet connection to download or distribute copyright material using peer-to-peer applications is strictly prohibited. Information Technology Services reserves the right to disconnect any machines involved in illegal file distribution from the College network.

Other Areas Prohibited

- Obscenity
- Pornography
- Copyright Infringement - It is violation of federal and state law to reproduce or distribute copyrighted material such as books, manuscripts, recorded sounds, and computer software. Computer users who copy, distribute (either free or for monetary gain), or receive copyrighted software of electronic information without paying the specified fee are in violation of U. S. Copyright laws.
- Threats and pranks
- Computer Security Violations - It is a violation of federal and state law to disrupt the integrity of another's computer system or to compromise any data integrity, confidentiality or availability, which includes obtaining unauthorized access to governmental computers, accessing a computer database to disrupt its normal function, or publishing, without authorization, a password, identifying code or other confidential information concerning a computer or database.

- Export Control Violations - Federal law limits the ability of persons to export encryption software to points outside the United States.
- Scams and Pyramid Schemes
- Circumventing software used to block certain Internet sites or maintain system security
- Attaching unauthorized equipment to the College network, including but not limited to wireless connections
- Using College-assigned network addresses without authorization
- Accessing, copying, modifying, transferring, or destroying other's information without permission
- Using the College seal or logo, or the photographs of any member of the College community without authorization
- Tying up resources through activities such as network gaming and mass e-mailing
- Employing the campus computer system in violation of the Policy 2.19--Honesty and Integrity--statement in the *Blue Mountain College Student Handbook* or standards specified in the *Blue Mountain College Employee Handbook*
- Tying up campus resources by using file-sharing programs
- Tying up campus resources by using streaming audio and/or video (radio, etc.)

3. **Reporting Violations**

Use of the College's computing facilities is a privilege not a right. Any member of the College community who witnesses or becomes aware of abuses of this policy should report them to the Director of Information Technology Services or the Office of Enrollment Services and Student Life. Policy violations may result in the immediate loss of the violator's computer and/or computing privilege and other disciplinary measures.

Before using the computing facilities, all students, faculty and staff will review and sign an Acknowledgment and Agreement of the *Acceptable Use of Technology Policy*.

4. **Protocol and Etiquette for Campus Email**

The College has developed protocol and etiquette for campus email, including the use of the campus listserve, which are included as part of the procedures for implementing this policy. All campus users of email are expected to follow these guidelines.

5. **Monitoring and Privileges**

A. Monitoring Tools

Blue Mountain College Information Technology Services routinely monitors usage patterns for its online communications to ensure online productivity and to support planning and management of network resources.

B. Blocking of Internet Access

Different accesses and service levels for different types of personnel may be given to employees depending on the nature of the work. The College reserves the absolute right to block access to certain internet sites at its discretion.

6. **Ownership of Electronic Communications**

A. College Ownership of Communications

All communications over the Blue Mountain College Online System are property of Blue Mountain College. The College reserves the right to monitor the Blue Mountain College Online System to attempt to ensure that any and all communications are in compliance with the stated mission and purposes of the College and assist with the safety of the College family.

B. Use of E-Mail

All faculty, staff, and students are expected to use good judgment when using the e-mail system. Sending chain e-mail or non-college-related mass e-mail violates this standard. Faculty, staff, and students should delete all chain e-mail and all non-college-related mass e-mail immediately upon receipt and refrain from further forwarding. Any references to any other entity in the email signature including other institutions of higher learning should be avoided by faculty, staff and students when using the e-mail system.

C. Non-Discrimination

The transmittal of messages with derogatory or inflammatory remarks about a person's race, color, sex, age, disability, national origin, physical attributes and sexual preference is prohibited.

7. **Maintaining System Security**

A. Keeping the Online System Secure from Computer Viruses and other Threats

Unauthorized downloading, uploading, or installing of software or files is prohibited. This is to prevent security threats from entering the college online systems. All software must be authorized by and registered to the Blue Mountain College. All software is to be approved and installed by the Office of Information Technology Services.

B. Unauthorized Use of Software

The use of unauthorized software is prohibited. All questionable software should be reported to the Office of Information Technology Services immediately for investigation and removal.

C. Other Unauthorized Downloads

No unauthorized downloads of service packs, software enhancements, or additions to authorized software is allowed without the approval of the Office of Information Technology Services.

SOURCE: Board of Trustees: February 26, 2010; October 02, 2009; October 03, 2008; October 07, 2005; October 01, 2004; October 04, 2002