MAINE COMMUNITY COLLEGE SYSTEM

GENERAL ADMINISTRATION
Section 203

SUBJECT: COMPUTER AND NETWORK USE

PURPOSE: To promote the responsible use of college and System computers and networks

As with any college system, the MCCS seeks to enhance opportunities for individual and collaborative learning and research. As a public institution with limited resources and distinct policy and legal obligations, the MCCS also needs to ensure that such uses are consistent with those resources and obligations. The goal of this policy is to balance these interests and promote responsible and secure use for all.

A. Application

This policy applies to:

1. Each college and other entity of the MCCS;

2. All computing resources owned or operated by the MCCS including, but not limited to, all hardware, software, peripherals, networks, network components, accounts, physical and logical data, e-mail and all other data or information transmitted by such equipment ("computers");

3. All employees, students and other persons who use such computers ("users"); and

4. In addition to any other computer use policy adopted by entities within the MCCS, and by entities outside the MCCS that operate resources accessed through or from the MCCS.

B. General Rules

1. Educational Priority

The priority use of MCCS computers is to provide direct support for learning, teaching and administration of MCCS programs. Such priority will govern access to MCCS computers.

2. Use is a Privilege, Not a Right

Use of MCCS computers and accounts thereon is a privilege, not a right. This privilege is limited by the provisions of this policy, any other pertinent policy or law, and may be withdrawn for violation thereof.

3. Limited Right of Privacy

Users may not have an expectation of privacy in their use of MCCS computers or networks. For example, the MCCS reserves the following rights:

a. Periodic Network Monitoring

The MCCS reserves the right to monitor periodically, randomly and without notice use rates, patterns, speed and system capacity to ensure the efficiency or integrity of the MCCS network and its computers. Such monitoring may proceed only by a person expressly authorized by the MCCS or college president;

b. Inspection of a Particular Account or Computer

The MCCS reserves the right to inspect those accounts, computers or files that the MCCS has reason to believe are misused, corrupt or damaged. Such inspection may proceed only by a person expressly authorized by the MCCS or college president and as advised by the MCCS general counsel; and

c. Access by Outside Agencies

User accounts, computers or files may also be subject to access in response to subpoenas, court orders, or other legal or regulatory requirements. Users will be notified as promptly as possible, unless notification is precluded by such subpoena or order.

4. Limited Designated Forum

The MCCS computer network constitutes a limited designated forum. This forum is designated for the limited purpose of helping students pursue, faculty to provide, and non-teaching staff to support the colleges' education, training and related programs.

5. Time, Manner and Place Limitations

The MCCS reserves the right to limit certain uses on or through the MCCS computers at those times and locations that the MCCS determines are necessary to regulate system capacity and speed. These limitations apply, but are not limited to, the downloading of video, music, photographic and other large data files.

6. Website and Webpage Development and Management

Any website, web page or other portion of a website hosted by a server owned, operated or maintained by a college or the MCCS is the property and speech of the MCCS, and the MCCS reserves all rights to control the access to, content of, and all other aspects regarding such web pages or websites. The Presidents Council may adopt a procedure for controlling the development and management of such web pages and websites, including standards controlling links to web pages and/or websites that are not owned, operated or maintained by a college or the MCCS.

C. Specific Prohibitions

Conduct that violates this policy includes, but is not limited to, the following:

1. Displaying, downloading, printing or distributing obscene, sexually explicit or sexually offensive images or text in a manner that constitutes sexual harassment or other violation of law;

2. Violating copyright laws, including the unlawful reproduction or dissemination of copyrighted text, images, music, video and other protected materials;

3. Using System computers for commercial activity, such as selling products or services;

4. Unauthorized access to or use of a computer, computer account or network;

5. Connecting unauthorized equipment to a college or MCCS network;

6. Unauthorized attempts to circumvent data protection or security including, but not limited to, creating or running programs that identify security loopholes or decrypt secure data;

7. Deliberately or negligently performing an act that will interfere with the regular operation of a computer;

8. Deliberately or negligently running or installing a program that, by intent or effect, damages a computer, system or network. This includes, but is not limited to, programs known as computer “viruses,” “trojan horses” and “worms;”

9. Deliberately or negligently wasting computing resources;

10. Deliberately or negligently overloading computing resources, such as running excessive programs that use relatively substantial bandwidth and other resources. This includes, but is not limited to, peer-to-peer applications;

11. Violating terms of applicable software licensing agreements;

12. Using electronic mail to harass or threaten another person or organization;

13. Initiating or perpetuating electronic chain letters or unauthorized mass mailings. This includes, but is not limited to: multiple mailings to news groups, mailing lists or individuals; "spamming;" "flooding;" and "bombing;"

14. Misrepresenting or misappropriating the identity of a person or computer in an electronic communication;

15. Transmitting or reproducing materials that are libelous or defamatory;

16. Unauthorized monitoring of another user's electronic communications; or reading, copying, changing or deleting another user's files or software without authority;

17. Communications that use public resources to promote partisan political activities;

18. Communications that are not otherwise protected by law because they constitute, for example, defamation, incitement to unlawful conduct, an imminent threat of actual violence or harm, fighting words, terrorist threats, gross disobedience of legitimate rules, criminal or severe civil harassment or false advertising; and

19. Otherwise violating existing laws or System policies.

D. Enforcement

Violation of this policy may result in the loss of computing and/or network access; other disciplinary action; and/or appropriate civil or criminal legal action.

E. Security

Upon recommendations of the college and System directors of information technology, the Presidents Council shall adopt a procedure that provides adequate uniform security for all System and college computers and networks.

REFERENCES: 20-A M.R.S.A. §12706(1)

DATE ADOPTED: June 24, 2009

DATE(S) AMENDED: