

# COMPUTER USE POLICY FOR ALL USERS

## GOVERNANCE AND ORGANIZATION

---

College Senate Chair:

President:

EMCC 205.7

Purpose: To promote and ensure the responsible use of computers by or through Eastern Maine Community College.

EMCC seeks to enhance opportunities for individual and collaborative learning and research. As a public institution with limited resources and distinct policy and legal obligations, EMCC 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.

### **Application:**

This policy applies to:

- A. each Center and any other entity of EMCC;
- B. all computing resources owned or operated by EMCC 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”);
- C. all employees, students and other persons who use such computers (“users”); and
- D. in addition to any other computer use policy adopted by entities of EMCC, and by entities outside EMCC that operate resources accessed through or from EMCC.

### **General Rules:**

#### **Educational Priority.**

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

#### **Use is a Privilege, Not a Right.**

Users do not have a right to use EMCC computers or accounts thereon. Users are granted a privilege to use such computers and accounts. This privilege is limited by the provisions of this Policy, any other pertinent policy or law, and may be withdrawn for violation thereof.

---

References: MCCS Policies #215  
Replaces: All previous publications

Effective Date: June 15, 2004  
Reviewed: 3/20/2009;

**Limited Right of Privacy.**

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

1. Periodic Network Monitoring. EMCC 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 EMCC network and its computers. Such monitoring may proceed only by a person expressly authorized by the college president.
2. Inspection of a Particular Account or Computer. EMCC reserves the right to inspect for reasonable cause those accounts, computers or files that EMCC has reason to believe are misused, corrupt or damaged. Such inspection may proceed only by a person expressly authorized by the college president and as advised by the MCCS General Counsel.
3. Search and Seizure by Law Enforcement Agencies. User accounts, computers or files may also be subject to search and seizure by law enforcement agencies for law enforcement purposes.

**Time, Manner and Place Limitations.**

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

**Examples of Specific Prohibitions**

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

- A. Unauthorized access to computers;
- B. Unauthorized use of a computer account;
- C. Connecting unauthorized equipment to the EMCC network;
- D. 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;
- E. Knowingly or recklessly performing an act that will interfere with the regular operation of a computer;

- F. Knowingly or recklessly 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”;
- G. Knowingly or recklessly wasting computing resources;
- H. Knowingly or recklessly 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.
- I. Violating terms of applicable software licensing agreements;
- J. Violating copyright laws, including their fair use provisions, through unlawful reproduction or dissemination of copyrighted text, images and other protected materials;
- K. Using System computers for commercial activity, such as selling products or services;
- L. Using electronic mail to harass or threaten another person or organization;
- M. 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”;
- N. Forging the identity of a person or computer in an electronic communication;
- O. Transmitting or reproducing materials that are libelous, slanderous or defamatory;
- P. Displaying, downloading, printing or distributing obscene, lewd, sexually explicit or sexually offensive images or text in a manner that constitutes sexual harassment or other violation of law;
- Q. Unauthorized monitoring of another user’s electronic communications; or reading, copying, changing or deleting another user’s files or software without authority; and
- R. Otherwise violating existing laws or EMCC policies.

**Enforcement**

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

**Security**

The EMCC Dean of Information Technology shall work with the MCCA Director of Finance and Administration to develop and adopt standards that provide adequate uniform security for all System computers and networks.

---

2/11/2009 updated titles only.