

# MUSC Computer Use Policy

This policy was approved by the MUSC Board of Trustees on October 12, 2001.

## Executive Summary

The University recognizes its legal and social obligations to respect the privacy of the authorized users of its computing and network resources. However, users must recognize that the confidentiality of their electronic communications cannot be guaranteed by the University. Moreover, the University reserves the right to audit or monitor any uses of its computing and network resources when necessary to ensure compliance with University policy, and with federal, state and local law.

The University network provides its authorized users with access to many classes of privileged information. Users must maintain the confidentiality and integrity of the information they access, and must not use privileged information for any purpose not explicitly authorized.

The University's computing and network resources exist to support the University's missions of teaching, research, patient care and public service. Incidental personal use of these resources by authorized users is permitted only to the extent that such use is lawful and ethical, does not conflict with the University's missions, does not interfere with other authorized users, and does not cause additional expense to the University.

## I. Introduction

The policy statements which follow serve primarily to aid in the interpretation of, and in a few cases to augment, the University's general policies on the appropriate use of University facilities, and the University's general ethics policies for faculty, students, and staff. At a minimum, faculty should refer to the Faculty Handbook, students to the MUSC Bulletin, and staff to the Medical University of South Carolina Human Resources Management Policy Manual for Non-Faculty Personnel ("the Personnel Manual"). The University's Intellectual Property Policy, which applies to faculty, students, and staff, may be found in the Faculty Handbook.

## II. Privacy and Confidentiality

In general, information stored on computers and the content of electronic communications are considered confidential, unless the owner or sender intentionally makes that information available to other groups or individuals. In particular, personal files on the University's computers (for example, files stored in a user's home directory, or on a personal computer) should be considered private to the same degree as personal files in University-assigned space in an office, lab, or desk area. Private communications via computer (for example, through electronic mail) have the same privacy protection as private communications via telephone.

Nonetheless, one should exercise caution when committing sensitive information to storage or transmission on any electronic media, because the confidentiality of electronic media cannot be

guaranteed. Confidential or sensitive information should not be sent through e-mail or exposed to public networks such as the Internet unless adequately secured against unauthorized access.

Routine maintenance can result in the contents of files and messages being seen by system or network administrators; however, network and system administrators are expected to treat the contents of electronic files and communications as private and confidential. Any inspection of electronic files or messages, and any action based upon such inspection, will be governed by all applicable US and SC laws and by this and other relevant University policies. Note also that under the Freedom of Information Act, the files of University employees (paper or electronic) may be considered public documents, and may be subject to inspection under the FOIA, through formal University-administered procedures. The content of electronic files and communications may also be subject to subpoena in other legal proceedings.

Moreover, the University reserves the right to monitor user activities on all University computer systems, and to monitor communications utilizing the University network, to ensure compliance with University policy, and with federal, state and local law. Monitoring shall be performed only by individuals who are specifically authorized, and only the minimum data necessary to meet institutional requirements shall be collected. Data collected through monitoring shall be made accessible only to authorized individuals, who are responsible for maintaining its confidentiality.

The following notice is understood to apply to all University-owned computer systems, and to all communications utilizing the University network:

This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized user may also be monitored. Anyone using this system expressly consents to such monitoring, and is advised that if such monitoring reveals possible evidence of illegal activity or violation of University regulations, system personnel may provide the evidence of such monitoring to University authorities and/or law enforcement officials.

### **III. Property Rights**

The ownership of the contents of electronic files and messages is a function of applicable US laws, State laws, and University and departmental policies. University contracts with third parties (for example, software license contracts and research and sponsored program contracts) may also apply.

The University's Intellectual Property Policy (see the Faculty Handbook) applies to all Inventions and Copyrightable Works produced by employees and trainees, including such works as may be embodied in electronic files.

### **IV. Academic Freedom**

Freedom to teach and freedom to learn are inseparable facets of academic freedom. The freedom to learn depends upon appropriate opportunities and conditions not only in the classroom, but on the

campus as a whole. The responsibility to secure and to respect general conditions conducive to the freedom to learn is shared by all members of the academic community -- faculty, staff, and students. System and network administrators are expected to respect the University's academic freedom policies.

No file stored on a University computer system should be removed by a system administrator without the file owner's permission unless the file's presence interferes with the operation of the system.

No posting to a University-sponsored electronic forum should be removed by a system administrator unless it violates US law, State law or University policy.

The following principles apply to University-supported electronic forums which support the free exchange of ideas among faculty and students (for example, Usenet news and Internet mailing lists):

1. The same standards of intellectual and academic freedom developed for faculty and student publication in traditional media apply to publication on electronic forums. Note that there are electronic forums and other materials on the Internet and elsewhere that some members of the University community may find offensive. The University cannot restrict the availability of such material, but the display of offensive material in any publicly accessible area, including but not limited to publicly accessible computer screens and printers, may violate other University policies on unacceptable behavior (for example, harassment or discrimination). Similarly, any use of University computing or network facilities to post offensive materials to electronic forums on the Internet and elsewhere may violate these University policies.
2. The authors of all postings submitted to electronic forums for distribution outside the University should include a disclaimer stating that the opinions expressed therein are not necessarily those of the University.

## **V. Responsibilities of Users**

All faculty, staff, and students who use University-supported computer and network systems share in the responsibility for upholding the rights of their fellow users. Meeting this responsibility requires adherence to certain rules, outlined below, which apply to all University systems.

### **A. Appropriate and reasonable use**

1. Computer and network access account should be used only for authorized purposes. Personal use of University computing and network resources is restricted by State law. [Section 8-13-700\(A\)](http://www.lpitr.state.sc.us/code/t08c013.htm) (<http://www.lpitr.state.sc.us/code/t08c013.htm>) of the South Carolina Ethics Code reads as follows:

No public official, public member, or public employee may knowingly use his official office, membership or employment to obtain an economic interest for himself, a member of his immediate family, an individual with whom he is associated, or a business with which he is associated. This prohibition does not extend to the incidental use of public materials,

personnel, or equipment, subject to or available for a public official's, public member's, or public employee's use which does not result in additional public expense.

2. Users should refrain from interfering with other users (for example, consuming gratuitously large amounts of limited system resources such as disk space, CPU time, or printer supplies.)

## **B. Privacy and Confidentiality**

1. Accounts on University computer systems, and connections to the University network, provide access to many classes of privileged information. Users must maintain the confidentiality of any privileged information they access, and must not use any privileged information for any purpose for which they are not explicitly authorized.
2. Accessing another user's files without permission is prohibited.
3. Accessing any information on a University information system without authorization is prohibited.
4. Disruption or unauthorized monitoring or interception of electronic communications is prohibited.
5. Use of any patient or other human subjects information for any research-related activity without Institutional Review Board (IRB) approval is prohibited.

These prohibitions apply even in circumstances where the files, information, or messages are not adequately protected against unauthorized access. Any user who discovers a possible "security hole" on an MUSC system is obliged to report it to the system administrator.

## **C. Accountability**

1. Misrepresenting or willfully concealing your identity at any point on the MUSC network is prohibited.

## **D. Security**

1. The users of all systems must maintain adequate passwords on their accounts. Passwords must be kept in strictest confidence, and may not be shared with others without the permission of the system administrator. If a user must temporarily share his or her password with a trusted system administrator (for example, to troubleshoot a problem), then the user should change the password as soon as possible afterwards. Note that passwords should never be shared with [anyone claiming to be] a system administrator without positive identification.
2. The users of all systems must comply with a system administrator's request to change passwords. Whenever possible users should choose their own passwords.
3. The users of all systems are responsible for understanding the system's default levels of protection applied to files and messages, and for supplementing that protection if necessary for sensitive information.
4. Any computer system which is connected to the University network must be maintained in accordance with generally accepted security principles. For example, virus protection

software must be installed and kept current, and any known security problems with the software installed on the system must be addressed.

5. All facilities for incoming remote access to computer systems and communication servers which are directly or indirectly connected to the University's campus-wide data communications network must provide adequate protection of other networked systems against unauthorized access. An audit trail of all remote access activity must be maintained by any facility which provides remote access, and audit trail records must be accessible by authorized University officials.

## **E. Copyright and Intellectual Property**

1. Copyrighted material and software must be used with respect for the legal rights of its copyright holder(s).
2. It is the user's responsibility to recognize, attribute, and honor the intellectual property present on or accessible through University computer and communication systems.

## **F. Licensed (Commercial) Software**

1. The user is responsible for understanding and adhering to the licensing terms for all licensed software which he or she knowingly uses.
2. The making of unauthorized copies of licensed software, even when the software is not protected against copying, is prohibited.

In addition to the above general rules, there are more specific rules which apply to many individual University systems. It is the user's responsibility to ascertain and follow these system-specific rules. For example, all MUSC patient care systems have very specific rules protecting the confidentiality of patient information, and external wide-area networks which you can access through MUSC's campus network often have somewhat restrictive "appropriate use" policies.

## **VI. Sanctions**

Violations of the MUSC Computer Use Policy by faculty, students, and staff are treated as violations of the applicable University ethics policies. Specific procedures for dealing with infractions (for example, disciplinary action and appeals processes) are detailed in the Faculty Handbook, the MUSC Bulletin, and the Personnel Manual.

Violations of public law which involve University computer and communication systems may be subject to prosecution by local, state or federal authorities.

University faculty, students, or staff who knowingly violate copyright and/or license terms (for example, by making or using an unauthorized copy of a copyrighted or licensed software product) may be personally liable for their actions.