

**SOUTHERN ILLINOIS UNIVERSITY
SCHOOL OF DENTAL MEDICINE
COMPUTER USAGE POLICY**

University owned or operated computing resources are provided for use by the faculty staff and students of Southern Illinois University School of Dental medicine (SIU-SDM). All faculty, staff and students have the responsibility to use the SIU-SDM computing resources in an effective, efficient, ethical and lawful manner. The following guidelines govern the use of these computing resources:

1. Computing resources and accounts are owned by the University, and are to be used for University-related activities only. All access to University owned computers and computing resources, including the issuing of passwords, must be approved and granted by the proper Administrative and Academic Computing Offices.
2. Computing resources and accounts are to be used only for the purpose for which they were assigned. They are not to be used for commercial purposes or non-university related activities. When the student enrollment or faculty/staff employment ends, use of computer resources and accounts must be terminated.
3. An account assigned to an individual, including Student Use accounts, must not be used by others without written permission from the SDM Office of Business Affairs. Faculty, staff and students are individually responsible for the proper use of their accounts, including proper password protection, logging in, logging out and appropriate use of Internet resources. Allowing friends, family or co-workers to use accounts, either locally or through the Internet, is a serious violation of these guidelines. Also, faculty, staff and students are responsible for choosing an appropriate password that adequately protects the security of the computing resources. They should periodically change their account passwords, particularly if someone may have seen the password being entered.
4. Programs and files are confidential, unless they have been explicitly made available to others by the owner. Network and File Server Administrators may access other's files when necessary for the maintenance of computing systems, or during investigation of serious incidents. The latter would require the approval by the appropriate university official, or as required by local, state, or federal law.
5. SIU-SDM computing resources cannot be used for inappropriate purposes and may not be altered. Such uses and alterations include but are not limited to:
 - a) Accessing pornographic or sexually explicit materials.
 - b) *Intimidation or creation of an atmosphere of harassment based upon gender, race, religion, ethnic origin, creed or sexual orientation. Fraudulent, threatening, abusive, profane or obscene e-mail or graphical displays used to harass or intimidate are prohibited and may be considered harassment.
 - c) Sending chain letters, mass mailings, broadcast messages, anonymous messages or repeated sending of e-mail after being requested to stop.
 - d) *Deliberately attempting to destroy or degrade the performance of a computer system (including network resources) by altering computer hardware or software to deprive authorized users of resources or access to any computer resource.

- e) *Using the network for financial gain or for any illegal activity, including violation of copyright, and ordering material to be sent with the intent of an unknowing party paying for it. This also includes using University modems to make unauthorized long distance calls.
 - f) *Using knowledge of loopholes in computer system security or unauthorized knowledge of a password to damage any computing systems, obtain extra computing resources, take resources from another user, gain access to computing systems or use computing systems for which proper authorization has not been given, either on-campus or off-campus.
 - g) Committing computer vandalism, which is defined as any malicious attempt to harm or destroy hardware, software or data of the university or of another user locally, through the network or the Internet. This includes, but is not limited to the uploading of, reaction or dissemination of viruses.
 - h) Wasteful use of resources such as printer paper and toner, as well as slowing or degrading network performance by excessive transfer of large files.
 - i) Customizing or modifying an operating system for personal use. This would include modifying or changing any files in a system folder or application folder on any university computer.
 - j) Using unauthorized personal software on any university computer without prior permission from the proper authorities. This includes but is not limited to computer games.
 - k) *Copying any copyrighted applications or files, not owned by the copier, from any university computers or file servers without permission from the owner of those files or applications.
6. For the protection of all SIU-SDM computer users, an individual's computer use privileges may be suspended or restricted immediately upon the discovery of a possible violation of these guidelines or other campus policies. Whenever possible, users whose computer access has been restricted or suspended will be notified of the restrictions and the means for resolving the matter.

Students who violate these guidelines will be subject to sanctions outlined in the Student Conduct Code. All cases will be referred to Student Conduct Committee.

Faculty or staff who violate these guidelines will be subject to disciplinary measures.

Violations of some of the above guidelines (*) may constitute criminal offense.

Approved: June 10, 1997