

Responsible Use Guidelines at Southern Illinois University School of Medicine

Introduction

Southern Illinois University School of Medicine provides extensive computing and network communication services for students, faculty, staff and individuals affiliated with the University. As a provider of these services, the University acknowledges that there is a shared responsibility between the users of these services and the network provider. The goal of this guideline is to establish a framework of accepted conventions regarding the use, management and governance of computing and network resources, while remaining cognizant of the principles of academic excellence to which the University continually strives.

This document constitutes the SIU School of Medicine guidelines for the management of computer networks, personal computers and the resources made available thereby. This guideline is intended to reflect the academic and ethical principles of the University community and indicates, in general, the privileges and responsibilities of those using University computing and network resources. A PDF copy of this document is kept on the Information Resources intranet site at http://www.siumed.edu/ir/Acceptable_Use.pdf.

Institutional Purposes

University computing and network communication services resources are to be used to advance the University's mission of education, research, and patient care. Faculty, staff, and students may use them only for purposes related to their studies, their responsibilities for providing instruction, the discharge for their duties as employees, their official business with the University, and other University sanctioned or authorized activities. The use of University computing resources and network communication services for commercial purposes including any sort of solicitation is prohibited, absent prior written permission of the appropriate University official(s). Use of University, computing resources for partisan political purposes is also prohibited.

Classification of Use

Decisions as to whether a particular use of computing and network resources conforms with this guideline shall be made by the Provost's Office if the use involves faculty or student academic matters, by the Office of Student Affairs if the use involves non-academic student use, and by the Department of Human Resources if the use involves administrators or staff.

Computing use shall include, but is not limited to, using University provided computers and networks or computer equipment to create, modify, manipulate or store files, information, or electronic media. This shall also include any creation, storage, manipulation or otherwise using electronic communications messages or email.

Cooperative Use

Computing resource users can facilitate computing at the University in many ways. Collegiality demands the practice of cooperative computing. It requires:

- Regular deletion of unneeded files from one's accounts on shared computing resources;
- Refraining from overuse of connect time, information storage space, printing facilities, processing capacity, or network services;
- Refraining from use of sounds and visuals which might be disruptive or offensive to others;
- Refraining from use of any computing resource in an irresponsible manner;
- Refraining from unauthorized use of departmental individual computing resources.

Impermissible Use

Computing resources may only be used for legal purposes and may not be used for any of the following purposes or any other purpose which is illegal, unethical, dishonest, damaging to the reputation of the University, inconsistent with the mission of the University, or likely to subject the University to liability. Impermissible uses (some of to which may also constitute illegal uses) include, but are not limited to, the following:

- Harassment;
- Libel or slander;
- Fraud or misrepresentation;
- Destruction of or damage to equipment, software, or data belonging to the University or others;
- Disruption or unauthorized monitoring of electronic communications;
- Violation of copyrights and software licensing agreements, or unauthorized copying or transmission of copyright-protected material;
- Unauthorized installation or use of software, and in particular, software which may create a security risk on University computer facilities;
- Use of the University's trademarks, trade names, logos, insignia, or copyrights without prior approval;

- Violation or attempted violation of computer system security;
- Unauthorized use of computer accounts, access codes(including passwords), or network identification numbers (including e-mail addresses) assigned to others;
- Use of computer communication facilities in ways that impede the computing activities of others (such as randomly initiating interactive electronic communications or e-mail exchanges, overuse of interactive network utilities, and so forth);
- Inspecting, modifying, distributing or copying data, or software without proper authorization, or attempting to do so;
- Inspecting, modifying, distributing or copying electronic mail messages without proper authorization or in a manner other than in the ordinary course of University business;
- Development or use of unapproved mailing lists;
- Use of computing facilities for personal or private business purposes absent prior written permission of the appropriate University official(s);
- Academic dishonesty, including but not limited to plagiarism and cheating;
- Violations under the Student Conduct Code, Faculty code of Ethics, or other University policies;
- Violation of network usage policies and regulations, or violation of usage policies and regulations of networks of which the University is a member or which the University has authority to use;
- Violation of privacy;
- Accessing, or attempting to access, another individual's or entity's data or information without proper authorization regardless of the means by which this access is attempted or accomplished;
- Posting or sending obscene, pornographic, sexually explicit, or offensive material;
- Posting or sending material that is contrary to the mission or values of the university;
- Intentional or negligent distribution of computer viruses;
- Concealing or misrepresenting user's name, affiliation or other identifier to mask irresponsible or offensive behavior or unauthorized use of identifier of other individuals or entities.

- General Policies

Access to and utilization of the computing resources and facilities provided by the University are a privilege and NOT a right; access to such resources and facilities may be withdrawn, limited, modified or curtailed if there is reason to believe that the user has or may have violated this guideline or applicable local, state or federal law. Additionally, violation of this guideline can result in further discipline under the appropriate processes and procedures set forth by the University or civil or criminal prosecution.

All users, as a condition of their access to or utilization of University computing or network services, agree to cooperate with and abide by University policies, regulations and guidelines, and applicable local, state and federal law. The user agrees to cooperate in an investigation of alleged improprieties or abuse of the privilege of using University computing services and waives any right of confidentiality. Any failure to cooperate fully with the University shall be considered a violation of this guideline.

Bandwidth to the internet is a limited resource. There can never be enough. Simply stated, if the use of the bandwidth is to promote the mission of the School, it will be allowed. The reason for these limitations is that the use of these methods limits the bandwidth available for Research and Education. There are no limits on using these methods for work related endeavors. There are three major categories of data transfer that are not permitted.

- Peer-to-Peer networking, commonly known as P2P is not permitted. If required to perform a Research or Educational function, it will be handled on a case by case basis. An example of this is the use of programs such as iMesh, Morpheus, Warex P2P, WinMX and Limewire. There are many other programs similar to these.
- “Streaming”. With the exception of work related uses, streaming audio and video is not permitted. Streaming audio and video is defined as such: *A technique for transferring data in a continuous flow to allow large multimedia files to be viewed or heard.* This definition is somewhat confusing. Basically, if you are listening to audio or watching a video that is brought to you via the internet, it is not allowed. Examples of this, but not limited to, would be the use of Windows Media Player, Real Player, QuickTime, Internet Radio, Yahoo Music, CNN broadcasts or movie clips.
- File transfers for the purpose of entertainment that are not using streaming protocols. An example of this would be the downloading an MP3 or MPEG file.

Responsibilities of Users

The user is responsible for correct and sufficient use of the tools available for maintaining the security of information stored on each computer system. The following precautions are strongly recommended:

- Users should not share computer accounts, passwords, and other types of authorization that are assigned to individual users with others;

- Users should assign an obscure account password and change it frequently;
- Users should understand the level of protection each computer system automatically applies to files and supplement it, if necessary, for sensitive or confidential information;
- Users should be aware of computer viruses and other destructive computer programs, and take steps to avoid being a victim or unwitting distributor of these programs;
- Users should take steps to insure their computer's operating system is kept up to date with all critical patches;
- Users should consider whether information distributed using University resources should be protected from unauthorized use by the use of copyright notices or by the restriction of distributing of certain materials to the Southern Illinois University users. Information regarding copyright may be obtained from the General Counsel's Office.

Security

The Southern Illinois University will assume that users understand and are aware that electronic files, data, and communications are not necessarily secure.

Users of electronic mail systems should be aware that electronic mail in its present form is generally not secure and is extremely vulnerable to unauthorized access and modification. The office of Information Technologies will make available to interested persons information concerning reasonable methods for attempting to protect information on central computing resources from loss, tampering, unauthorized search, or other access. Level of obtainable security will vary depending upon the system involved. Information of procedures appropriate to each resource will be available in the Information Technology office, Security Officer,

Privacy and Confidentiality

The University reserves the right to inspect and examine any University owned or operated communication system, computing resource, and/or files or information contained therein at any time, subject to the terms and conditions contained herein (viewing information in the course of normal system maintenance does not constitute disclosure).

Outside sources

When sources outside the University request an inspection and/or examination of any SIU owned or operated communication system, computing resource, and/or files or information contained therein, the University will treat information as confidential unless any one or more of the following conditions exist:

- When approved by the appropriate University official(s) of the head of the Department to which the request is directed;
- When authorized by the owner(s) of the information;
- When required by federal, state, or local law;
- When required by a valid subpoena or court order;

Note: When notice is required by law, court order, or subpoena, computer users will receive prior notice of such disclosures.

Internal sources

The Provost, Vice Chancellor of Student Affairs, or the Director of Human Resources, or their designees, may direct that an inspection and/or examination of any University owned or operated communication system, computing resource and/or files or information contained therein when:

1. the inspection and/or examination serves a legitimate University purpose; and/or
2. there is a reasonable suspicion that the inspection and/or examination will reveal a violation of local, state, or federal law.

The applicable University grievance policy is available to anyone who has been aggrieved by the decision of the Provost, Vice Chancellor of Administration, or Director of Human Resources.

External Networks

It is expected that all members of the University community will abide by the guidelines and policies set forth herein while pursuing University business, wherever located. Members of the University community who use networks, facilities, or computers not owned by the University shall adhere to this Acceptable Use Guideline and all policies and procedures established by the administrators of non-University networks, facilities, or computers they use (policies and procedures can usually be obtained from the network information center of the network in question). Whether or not an external guideline exists, this Acceptable Use Guideline shall remain in effect and shall be adhered to by members of the University community at all times.

Software Piracy Policy Statement

Respect for the intellectual work and property of others is vital to the mission of higher education. This principle applies to works of all authors and publishers in all the media, including labor and creativity resulting in computer software. It encompasses respect for the right to acknowledgement and the right to determine the form, manner, and terms of publication and distribution.

It is the policy of Southern Illinois University that unauthorized copying of computer software will not be tolerated. Such copying is both unethical and illegal. University employees and students making, acquiring or using unauthorized copies of computer software may be subject to University disciplinary sanctions as well as legal action by the copyright owner.

Electronic Mail/Communications

Electronic mail and communication have become an integral part of society, and have become indispensable to the members of the University community. Users should be aware of the weak privacy afforded by electronic communications and electronic data storage. Users should not commit confidential information to either, and understand that there is no expectation of privacy in such communications.

Electronic mail and other forms of communication should be used in responsible and courteous manner. Use of electronic mail, other communications services, or other network communications facilities to harass, offend, or annoy other users of the network is forbidden. All users need to be aware that material which is obscene, defamatory, or violates University guideline on non-discrimination will not be tolerated. The University reserves all rights to take appropriate measures to prevent, correct, or discipline behavior that violates this guideline.

Electronic mail communications which on University networks or equipment, including, but not limited to, electronic mail and personal information, is subject to examination by the University when:

1. It is necessary to maintain or improve the functioning of University computing resources;
2. there is a suspicion of misconduct under University policies, or suspicion of violation of local, state, or federal laws; or
3. It is necessary to comply with or verify compliance with local, state, or federal law.

If the University inadvertently discovers messages or data files within its network that lead it to suspect the presence of illegal activities or activities which violate University policies, then the University will be free to use that discovered information to pursue investigations or inform the appropriate authorities.

Sanctions

Violations of this Guideline shall subject users to the regular disciplinary processes and procedures of the University for students, staff, administrators, and faculty and may result in loss of their computing privileges. Illegal acts involving University computing resources may also subject violators to prosecution by local, state, and/or federal authorities.

Disclaimer

As part of the services available through the campus network, the University provides access to a large number of conferences, lists, bulletin boards, and Internet information sources. These materials are not affiliated with, endorsed by, edited by, or reviewed by the University, and the University takes no responsibility for the truth or accuracy of the content found within these information sources. Moreover, some of these sources may contain material that is offensive or objectionable to some users.

Existing University Rules and Regulations

This guideline is intended to be an addition to existing University rules and regulation and does not alter or modify any existing University rule or regulation.

Revision History

| | | |
|-----------------|-----|--|
| 15 October 2004 | REF | Acceptance by IMPC |
| 16 June 2005 | REF | Added Revision History to the document |
| 21 July 2005 | REF | Added definition of streaming. Many people do not understand what this is. |