POLICY GOVERNING THE USE OF COMPUTING AND NETWORK RESOURCES

At Saint Joseph's University
Revised December, 2008

Mission Statement

To support the missions of teaching, research, and public service, Saint Joseph's University provides access to computing and information resources for students, faculty, and staff, within institutional priorities and financial capabilities.

General Requirements

All members of the University community who use the University's computing and information resources must do so responsibly. Every user is responsible for the integrity of these resources. All users of University-owned or University-leased computing systems must respect the rights of other computing users, respect the integrity of the physical facilities and controls, and respect all pertinent licenses and contractual agreements. It is the policy of Saint Joseph's University that all members of its community act in accordance with these responsibilities, relevant laws and contractual obligations, and in the highest standard of ethics.

Computing facilities and accounts are owned by the University and are to be used for the University-related activities for which they are assigned. University computing resources are not to be used for commercial purposes or non-University-related activities without written authorization from the University. In these cases, the University may require payment of appropriate fees. This policy applies equally to all University-owned or University-leased computers.

The University reserves the rights to limit, restrict, or extend computing privileges and access to its information resources. Data owners--whether departments, units, faculty, students, guests or staff--may allow individuals other than University faculty, staff, and students access to information for which they are responsible, so long as such access does not violate any license or contractual agreement; University policy; or any federal, state, county, or local law or ordinance.

Users and system administrators must guard against abuses that disrupt or threaten the viability of all systems, including those at the University and those on networks to which the University's systems are connected. Access to information resources without proper authorization from the data owner, unauthorized use of University computing facilities, continued overuse of resources that degrades system performance, and intentional corruption or misuse of information resources are direct violations of the University's standards for conduct as outlined in the Saint Joseph's University Policy Manual, the Personnel Policies and Procedures for Professional and Salaried Staff, the Faculty Handbook, and the Official Student Handbook and may also be considered civil or criminal offenses.

Saint Joseph's University treats policy violations of computing facilities, equipment, software, information resources, networks, or privileges seriously. Disciplinary action is described in the section Penalties for Misuse of Computing and Information Resource Privileges.

System Administrator Responsibilities

- Maintain size limits on user file systems and incoming email systems. These limits will change from time to time.
- Detect weak passwords and contact users to change them to a stronger password.
- Scan the network file systems for viruses and remove them. Notify users who repeatedly have viruses in their file space.

- Investigate reports of problems caused by users on Saint Joseph 's network to internal or external computers or networks.

User Responsibilities

If you or your guest use the University's computing resources or facilities, you have the following responsibilities in addition to those described in the preceding sections:

- Use only those computer services, networks and accounts which the University has authorized for your access.
- Use accounts only for the purpose(s) for which they have been issued.
- Be responsible for all use of your accounts and for protecting each account's password. Users are not allowed to divulge computer account passwords. Passwords should consist of a mix of 7 or 8 alphanumeric characters, and should be changed frequently throughout each semester of use. Do not use easily identifiable personal information such as names, telephone numbers, birth dates, etc.
- Immediately report unauthorized use of your accounts to the Office of Information Technology.
- University communications systems (electronic mail, electronic messaging, and similar services) may not be used for unlawful purposes or purposes that violate other University policies. The latter include, but are not limited to, sexual or other forms of harassment. Electronic communication may not be used for commercial purposes except under the direction of the University.
- Ensure that all software that you use is properly licensed. Do not use or share unlicensed software including computer programs, music files and other digital media. The unauthorized sharing of music files and other digital media is a violation of the Digital Millennium Copyright Act and you are potentially liable for damages. Take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on any system, network, or server that you operate.
- Cooperate with system administrator requests for information about computing activities. Under certain unusual circumstances, a system administrator is authorized to access your computer files.
- You are held responsible for the actions of your guest(s). Violations of computing resource policy committed by any guest will be attributed to that guest's sponsor.
- You are responsible for making backup copies of your documents and personal software.
- The use of electronic mail is to be treated as the use of postal services. Email messages are to be opened and read by the user to whom they are addressed. Do not attempt to read, delete or otherwise tamper with email addressed to another user. Do not attempt to distort or forge the "address" information of email messages. Do not send harassing or offensive email.
- You may not attempt to gain control of any files or computers without the prior consent of the "owner" of those files. The system administrator does not give consent for users to attempt to gain control of any network servers, routers, or switches. The system administrator does not give consent for users to "look around" the file systems on any server.

If you are a project director for a group of computing users, a supervisor whose staff use computers, or a faculty member whose students use computers, you must help your project members, staff or students learn more about ethical computing practices and promote good computing practices and data management.

As an aid to a better understanding of responsible computing practices, all departments that own or lease computing equipment are encouraged to develop "Conditions Of Use" documentation for all systems that they operate and to make these "Conditions Of Use" documents available to users. These documents should be consistent with the

policies and procedures set forth by the Office of Information Technology (for example, the *Policy Governing Computing and Network Resouces at Saint Joseph's University*) and should be approved by the department's administrative officer or other individual designated by that administrative officer.
The University is not responsible for loss of information from computing misuse, malfunction of computing hardware or software, external contamination of data or programs. The staff in Information Technology units such as Network Services and all other system administrators must make every effort to ensure the integrity of the University's computer systems and the information stored thereon. However, users must be aware that no security or back-up system is 100 percent foolproof.

Penalties for Misuse of Computing and Information Resource Privileges

Abuse of computing resources is subject to disciplinary action. If the Office of Information Technology has a sufficiency of evidence to indicate that intentional or malicious misuse of computing resources has occurred, and if that evidence points to the computing activities or the computer files of an individual, any or all of the following steps will be pursued to protect the user community:

- Notify the user's project director, instructor, academic advisor, or administrative officer of the investigation.
- Refer the matter for processing through the University's judicial system.
- Suspend or restrict the user's computing privileges during the investigation, including inspecting that user's files, diskettes, and/or tapes. Disciplinary action may include the loss of computing privileges and other disciplinary sanctions up to and including non-reappointment, discharge, dismissal, and legal action. In some cases, an abuser of the University's computing resources may also be liable for civil or criminal prosecution under Title 18 PA C.S. @5742 (1990), or other appropriate legislation.

It should be understood that nothing in this policy precludes enforcement under the laws and regulations of the Commonwealth of Pennsylvania, any municipality or county therein, and/or the United States of America.

All computer users are urged to become familiar with the University Policy of Academic Honesty as it pertains to the use and abuse of University computer resources, as well as the *Policy Governing the Computing and Network Resources at Saint Joseph's University*. Any observed violations of these policies must be reported to the appropriate administrative officers and to the Office of Information Technology.

Use of Unlicensed Software

All software installed on the University's computer systems must be properly licensed, either by the University, or by the individual user. The University will monitor its computer systems to ensure that unlicensed software is not installed on its computers. Individuals who install software on their office computers must keep records to show that this software is properly licensed, and they must inform Information Technology that the software has been installed.

Compliance with Copyright Laws for Text, Audio and Video

Nearly all written, audio and video material is protected by copyright laws, regardless of whether it is in a hard copy, in an electronic copy, or on the Internet. The exceptions to this rule are so few that users of SJU technology should assume that all written audio and video materials in hard copy or available through the Internet are protected by copyright laws, including The Digital Millennium Copyright Act of 1998, unless there is clear information to the contrary. Simply stated, the copyright laws allow a user to read the copyrighted material. The copyright laws do not allow a user to modify a copyrighted work, make copies of it (beyond those allowed by fair use), distribute copies of a work through the Internet, or broadcast a copy of a work (such as in the case of video) on any channel or network. As with materials from a library or other sources, the user is responsible for using materials obtained off the Internet in compliance with the copyright laws.

Compliance with Copyright Laws for Software

Nearly all computer software is protected by the copyright laws. The exceptions to this rule are so few that users of SJU technology should assume that all software on a SJU computer system, on third party systems, or available through the Internet is protected by copyright, unless there is clear information to the contrary. Simply stated, the copyright laws allow a user of software to use the software, load it onto the hard drive of a computer, and retain the original disk as an archive copy. The copyright laws do not allow a user to modify the software, make more copies of it, store copies on both a home and a campus computer, or distribute the software through the Internet, unless the license agreement permits those activities. Unless a user of SJU computer systems knows that any of those activities is permitted by the applicable license agreement, users of SJU computer systems shall not copy any software, modify any software, load copies of it onto a network or on multiple hard drives, or distribute the software in any way, including through the Internet.

Policy Revision Date: Thursday, December 18, 2008