

N.B.: Seton Hall University reserves the right to amend or otherwise revise this document as may be necessary to reflect future changes made to the I.T. environment. You are responsible for reviewing this Policy periodically to ensure your continued compliance with all Seton Hall University I.T. policies.

1. **Policy Title:** Seton Hall University Appropriate Use of Information Technology Policy.
2. **Audience:** All users of Seton Hall University's campus computing, telecommunications, document services, educational media, and management information systems technologies. These I.T. resources support the instructional, research, and administrative activities of the University.
3. **Policy Statement:** Because of the broad impact and potential liabilities for the inappropriate use of Information Technology, all users of Seton Hall Information Technology Resources, by the simple act of using any of them, agree and are bound to abide by the following guidelines.
4. **Definitions:**
 - a. Information Technology (I.T.) at Seton Hall University encompasses the use of all campus computing, telecommunications, document services, educational media, and management information systems technologies. These I.T. resources support the instructional, research, and administrative activities of the University. Examples of these resources include, but are not limited to, the central administrative, academic and library computing facilities; the campus-wide data, video and voice network; electronic mail; video conferencing systems; access to the Internet; voice mail; the University switchboard; fax machines; photocopiers; classroom audio-video; departmental and general use computing facilities and related services.
 - b. Appropriate Use of I.T. Resources. Users of these services and facilities have access to valuable university resources, to sensitive data and to external networks. Consequently, it is important for all users to behave in a responsible, ethical and legal manner. In general, appropriate use means understanding the intended use for Seton Hall I.T. (and making certain that your use complies); respecting the rights of other Seton Hall information technology users; maintaining the integrity of the physical facilities, and obeying all pertinent license and contractual agreements.
 - c. Guidelines. This document establishes general guidelines that apply to all users of I.T. resources owned or managed by Seton Hall University, including but not limited to Seton Hall students, faculty, staff, external individuals (such as Seton Hall contractors) or organizations and individuals accessing external network services, such as the Internet, via Seton Hall's Information Technology facilities.
 - i. The policies described in this document apply to all information technology owned or managed by Seton Hall University and represent the minimum appropriate use policies for I.T. Individual departments may have additional (and more restrictive) policies regarding I.T. resources held in those departments.
 - ii. Departmental users should contact their Information Technology Liaison person for more information about I.T. policies in a specific department. It is strongly recommended that

each department appoint at least one Information Technology Liaison person designated to provide first level I.T. support, receive training with the UITS organization; and exchange pertinent I.T. information between UITS and the department.

d. Users' rights.

i. Access to I.T. Resources

1. Central I.T. Resources Undergraduate and graduate students, faculty, administrators, staff and recognized student organizations may obtain IDs for use with the central I.T. activities related to instruction, research or university administration.
2. In the event that any student, faculty, administrator or staff person leaves, resigns or in any way concludes his or her relationship with Seton Hall University for whatever reason:
 - a. access to all I.T. resources, including voice mail and email services, will be terminated immediately
 - b. all electronic storage will be deleted.

ii. Other I.T. Resources. Most of Seton Hall's I.T. facilities and services—such as the Computer Resource Centers, the Computer-Equipped Classrooms, Video Conferencing rooms, consulting services, voice mail, and training—are available to members of the University community. UITS plans and budgets for central I. T. services. However, these services are not free. Users/departments may be required to fund the additional expense of excesses (based on historical, normal utilization) or abuses of Seton Hall I.T. resources (expenses beyond the baseline budget).

iii. Departmental I.T. Resources For information concerning access to departmental I.T. resources, contact your department's Information Technology Liaison or Department Chair.

e. Data Security and Integrity.

i. UITS-Maintained Equipment

1. UITS provides reasonable security against intrusion and damage to files stored on the central I.T. facilities. UITS also provides some facilities for archiving and retrieving files specified by users and for recovering files after accidental loss of data. However, other users can hold neither the University nor any I.T. staff member accountable for unauthorized access, or can they guarantee protection against media failure, fire, floods, etc. Users should use all available methods to protect their files, including use of strong passwords, the periodic changing of their passwords, backing up important data on a regular basis and storing back-up copies of information off site. In the event that data have been corrupted as a result of intrusion, UITS should be notified immediately. Every reasonable attempt will be made to restore files to their status prior to intrusion; however, UITS cannot guarantee restoration. Users should not store any University confidential information on external storage devices and or personal computers.
2. Upon request, the I.T. staff will assist in implementing procedures to maximize security. Although UITS backs up some departmental servers and makes reasonable

attempts to protect those servers from intrusion, it does not provide the same level of protection or offer restoration of files stored on departmental servers. Therefore, it is especially important that users back up their files and use all available means to protect their data on departmental systems.

3. Seton Hall University Information Technology Services, UITs, reserves the right to manage the University's voice, data and video bandwidth. Criteria for bandwidth management involves the integrity and robustness of university-owned equipment, data, and services as well as the appropriateness of bandwidth use when compared to the University's academic goals, administrative missions, and appropriate use policy for information technology.
 - ii. Departmental Facilities. Data security and integrity in departmental I.T. facilities varies depending on the department. Users should contact their department's INFORMATION TECHNOLOGY LIAISON for more information on their security and data integrity procedures.
- f. Privacy.
- i. Access by I.T. Staff on Behalf of the University. Although not legally required to do so, the University respects the privacy of all users. Members of the UITs organization are forbidden to log on to another user's account or to access a user's files unless the user gives explicit permission (for example, by setting file access privileges). Exceptions to this privacy policy are made, however, under specific conditions. Such conditions include investigation of programs suspected of causing disruption to the network or other shared services; investigation of suspected violations of state or federal law or university policies; and investigations to avoid liability or in connection with internal hearings or litigation. In these instances, the Chief Information Officer and the Information Security Officer upon consultation with University Counsel must be convinced that there is sufficient cause to review files before those files can be searched without the user's permission.
 - ii. Before logging onto a user's account or accessing a user's private files, a reasonable attempt will be made to contact the user to inform him or her that UITs will access the files. If that is not possible, the Chief Information Officer will view the files for the suspected violation and will inform the user afterward that the files have been reviewed. Information obtained in this manner is admissible in legal proceedings or in a university hearing. In accepting a user account, the user agrees to this policy.
 - iii. Access by Administrators of Departmental I.T. Systems. The administrators of departmental I.T. systems, such as INFORMATION TECHNOLOGY Liaisons, should not access a user's files without the explicit permission of that user or monitor file traffic at a level that will permit intrusion into the file contents. However, some exceptions may be necessary, for example, when a file is suspected of causing disruption to a local network or other shared services and a user cannot be reached.

- iv. Furthermore, information about system users and information stored by them should be treated as confidential. Individual departments may have guidelines consistent with university policy which deal with access issues of their I.T. resources.
- v. Electronic Communications
 - a. Users should not use personal e-mail to conduct University business.
 - b. Users should not expect privacy of any electronic communications. I.T. systems' administrators may see the contents of electronic communications due to serious addressing errors or as a result of maintaining the communications system. In those cases where administrators do see the contents of private electronic communications, they are required to keep the contents confidential. Users should also be aware that the current design of the networks is such that the privacy of electronic communications that leaves Seton Hall cannot be guaranteed.
 - c. Also, when a user's affiliation with Seton Hall ends, e-mail subsequently received at Seton Hall that is addressed to the former user will either be returned to the sender or, if appropriate, forwarded for an agreed upon limited time, to an address specified by the former user
- g. Ownership of Copyright for Materials Developed with Seton Hall's Resources. Seton Hall University has established guidelines related to ownership of copyright property. The exact policies and procedures relating to copyrights may be obtained from the office of University Counsel.
- h. Responsibility for Errors in Software, Hardware, and Consulting. UITs, in conjunction with department Information Technology Liaison, makes its best effort to maintain an error-free I.T. environment for users and to ensure that the I.T. staff is properly trained. Nevertheless, it is impossible to ensure that I.T. system errors will not occur or that I.T. staff will always give correct advice.
- i. Seton Hall presents no warranty, either expressly stated or implied, for the services provided. Damages resulting directly and indirectly from the use of these resources are the responsibility of the user. However, at the request of the user, when errors are determined to have occurred on I.T. facilities, members of the I.T. staff will make a reasonable attempt to restore lost information to its state prior to the failure, at no cost to the user.
- j. As part of maintaining the I.T. environment, the I.T. staff applies vendor-supplied or locally developed fixes as appropriate when problems are identified.
 - i. Given that vendors may be involved and that staff resources are finite, no guarantee can be made as to how long it may take to fix an error once it has been identified.
 - ii. When software errors are considered major problems or could produce inaccurate results, users will be notified as soon as possible using appropriate electronic and/or other media.
- k. Changes in the Seton Hall I.T. Environment. When significant changes in hardware, software or procedures are planned, Information Technology Liaison Officers will notify their departmental user community through electronic mail and other media to ensure that all users have enough time to prepare for the changes and to voice any concerns that they might have.

1. Computer Abuses - You can expect to lose your computer account, be disconnected from the network, have your web page removed, face disciplinary action up to and including termination, possibly be charged with criminal offenses or have civil action taken for computer abuses such as:
 - i. Unauthorized access of another person's computer or email account
 - ii. Unauthorized access of University data or systems
 - iii. Misrepresenting either the University or your role at the University to obtain access to data or computer systems
 - iv. Attempting to intercept any network communication for purposed including but not limited to: reading message/file content; rerouting packets; or packet sniffing
 - v. Using computing resources to access any other computer system (on or off-campus) without authorization
 - vi. Disseminating any confidential information unless such dissemination is required by the individual's job at the University
 - vii. Deleting or copying files from another person's computer account
 - viii. Taking advantage of another user's naive to gain access to his/her files
 - ix. Preventing someone from using his/her account by changing the password or other tampering
 - x. Sending offensive, harassing or threatening messages or repeated unsolicited mail
 - xi. Abusing the networks to which the University belongs
 - xii. Use of the computer or network for monetary gain, political purposes or illegal activities
 - xiii. Illegal use of downloaded copyrighted materials including print, audio, and video
 - xiv. Intentionally writing, producing, generating, copying, propagating or attempting to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software unless such action is part of authorized research or testing. Such software is often referred to as a virus, worm, Trojan Horse, or some similar name
 - xv. Illegally distributing copyrighted software within or outside the University through any mechanism, electronic or otherwise
 - xvi. Using University data or computing resources/systems to violate state or federal laws/regulations
 - xvii. Performing or assisting in the performance of any act that will interfere with the normal operation of computer, terminals, peripherals, networks, or in any activity that interferes with the rights of others such as writing/releasing viruses

5. Policy Statement: Guidelines for Appropriate Seton Hall I.T. Use

The following list, while not exhaustive, provides some specific guidelines for appropriate I.T. use:

- a. Use Seton Hall's Information Technology facilities and services for Seton Hall University related-work, not for personal or other-than-Seton Hall business work. Pay particular attention to abuse of photocopiers, local and long distance phone calls, fax machines, the Internet and the local Seton Hall networks.
- b. Seton Hall University encourages information technology literacy for its students, faculty and staff. As such, Seton Hall University allows its electronic mail system and personal World Wide Web pages to be used by students, faculty and staff for reasonable and limited personal use. For example, occasionally sending electronic mail to family and friends is allowed, as is the hosting of a personal web page. In all cases this "personal use" must conform to the guidelines established herein, dealing with the prohibition of personal, financial gain.
- c. Use only the Information Technology facilities for which you have specific authorization. Do not use another individual's ID or account, or attempt to capture other users' passwords. Users are individually responsible for all use of resources assigned to them; therefore, sharing of IDs is prohibited.
- d. Observe established guidelines for any information technology facilities used both inside and outside the University. For example, individuals using Seton Hall's Computer Resource Centers must adhere to the policies established for those centers; individuals accessing off-campus computers via external networks must abide by the policies established by the owners of those systems as well as policies governing use of those networks.
- e. Do not attempt to alter, delete or destroy any software on any Seton Hall I.T. system. This constitutes a violation of appropriate use of I.T. facilities no matter how weak the protection is on those products.
- f. Do not store any University confidential Information on to external storage devices and or personal computers.
- g. Your use of Seton Hall I.T. facilities and services is subject to and conditional upon your compliance with state and federal laws and university policies, including disciplinary policies.
- h. Respect the privacy and personal rights of others. Do not access or copy another user's electronic mail, data, programs, or other files without permission. Seton Hall endorses the following statement on software and intellectual rights distributed by EDUCAUSE, the non-profit consortium of colleges and universities, committed to the use and management of information technology in higher education. The statement reads:
 - i. Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to work of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy and right to determine the form, manner and terms of publication and distribution.
 - ii. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of

authorial integrity, including plagiarism, invasion of privacy, unauthorized access and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

- i. The official Seton Hall University position on peer-to-peer (P2P) file sharing utilities (e.g., KaZaa, iMesh, Gnutella, etc.) is that the software itself is not illegal, nor banned by Seton Hall University. It is illegal, however, to download or share copyrighted material for which you do not hold the copyright.
- j. You are expected to comply with the Information Security Policy that establishes expectations and directives to address risks associated with the University's computing and information resources and to protect Seton Hall's information resources from accidental or intentional unauthorized access or damage, while supporting the mission statement requirements of its academic culture.
- k. You are expected to abide by all applicable copyright laws and licenses. Both University policies and the law expressly forbid the copying of software that has not been placed in the public domain and distributed as "Freeware" or "Shareware". Users are expected to abide by the requirements of shareware agreements. Each individual department or department IT Liaison is responsible for keeping records and original licenses of departmental software installed on office systems. UITS will maintain university-wide site licenses.
- l. Recent rulings by the courts under the Digital Millennium Copyright Act have held that Internet Service Providers or ISPs (e.g. Seton Hall University is an ISP to its students, faculty and staff) must provide the identity of users of specific Internet Protocol Addresses or "userids" of the programs listed above when a properly issued subpoena is provided. Individual students, faculty and staff may be held personally liable for violations of copyright laws.
- m. The University policies on plagiarism or collusion apply to uses of I.T. resources in course assignments.
- n. In order to avoid jeopardizing the University's tax-exempt status, do not use Seton Hall I.T. facilities and services for personal financial gain or in connection with political activities, without prior written approval in each instance.
- o. Use appropriate standards of civility and common sense when using I.T. systems to communicate with other individuals. Do not use e-mail to transmit confidential information relative to personnel matters, internal investigations and litigation. When sending personal messages to other users, participating in a Chat Room discussion, posting on electronic bulletin boards or leaving a voice mail message, identify yourself as the sender. Using Seton Hall's I.T. resources to harass, slur, embarrass or demean other individuals are explicitly prohibited.
- p. Be sensitive to the needs of others, and use only your fair share (what a reasonable person would consider fair) of computing, faxing, dial-up networking and telephone resources. For example, users of shared resources, such as Seton Hall dial up Internet connections or the PCs in the Computer Resource Centers, should use these facilities for only the most essential tasks during periods of peak demand. Broadcasting non-critical messages to large numbers of individuals (spamming) and sending chain letters are examples of activities that cause network congestion and interfere with the

- work of others, and are prohibited. Use the available online and telephone company directories to look up the numbers your-self to save the University additional telephone service charges.
- q. Treat I.T. resources and electronic information as a valuable university resource. Protect your data and the systems you use. For example, back up your files regularly. Set an appropriate password and change it regularly. Passwords should not be any easily remembered word or phrase. Select a random string of letters and numbers with a recommended length of at least 8 characters (if the system allows). Make sure you understand the access privileges you have set for your files. Do not destroy or damage any I.T. equipment, networks or software. The willful introduction of computer code that compromises the integrity of a system, such as viruses and worms, into the Seton Hall University computing environment or into other computing environments via Seton Hall's network violates university standards and regulations. This may result in a range of penalties from termination of user access to Seton Hall I.T. resources to expulsion/removal from the University.
 - r. Stay informed about the Seton Hall I.T. environment, as it is continually evolving to keep Seton Hall with academia and the demands of our students. Seton Hall disseminates information in a variety of ways, including the UITS Announcement page on the Web, the Seton Hall Home Page, logon messages, the Information Technology Liaison listserv, and online documentation regarding software policy and procedures; in published newsletters (e.g., Seton Hall Press); at meetings; and, in some cases, as announcements/memos mailed to departments/individuals. Users are responsible for staying informed about these changes and are expected to adapt to changes in the University I.T. environment.

6. Background Issues:

Policies such as this “Appropriate Use of Information Technology” are created by the Seton Hall leadership to insure compliance with relevant legislation and regulations as well as to help Seton Hall achieve its goals. It is vitally important that such policies be widely understood and enforced.

7. Financial Issues:

Liability from potential lawsuits and compromises of Personally Identifiable Information

8. Comments, Suggestions, Corrections, etc.

Questions concerning this or any other Information Technology Policy can be directed to UITS Helpdesk.