University of Scranton
Student Computing Policy

Students are responsible for reading, understanding, and abiding by this policy.

I. Electronic Resources at the University

Information resources can help you be more productive as a student -- to produce papers, to use the library catalog, to send messages to your professors and friends, to access class notes and assignments, and to conduct the general business of student life. The University makes information resources available to you in many ways:

- Everyone at the University has access to information servers for electronic mail (e-mail) and other Internet services.
- The University's web sites contain information to help you register for classes, apply for financial aid, keep up with University events, and much more.
- Microcomputers are available for general use at locations around the campus. These microcomputer sites provide access to the Internet and essential software for coursework.
- You can drop and add courses and check semester grades and other related information by using the Web.
- Selected classrooms, labs, and library carrels are equipped with data outlets for Internet access.
- There are data network connections in all University-owned houses and residence hall rooms to connect your personal computer to the Internet.

II. Use and Ownership

We will use the possessive word "your" a lot in this policy, but this does not always mean ownership. In some cases, it means "exclusive use." You may own a personal computer or workstation. You will make the decisions about how that equipment will be used. You may own a software license -- word processing or spreadsheet software, perhaps -- which you purchased from a software vendor. Your license usually allows you to possess one copy of this software for your own use.

The University owns the central computers, departmental computer labs, the microcomputing sites, the computers it places in its offices, and all the software it has installed on them. The University determines who may use these resources and how they may use them.

The University owns the University network -- all the wires, cables and routers that connect the central computers, computer labs, microcomputer sites and perhaps your personal computers to each other
and, beyond the campus, to the Internet. The University determines who is authorized to use its network, and can limit the nature of the use.

III. Internet Guidelines

- Be aware of the thousands of others who rely on the University’s computers to do their work. Consider how your computer behavior will affect them and choose what you know is right.

- Understand that University policies that address academic dishonesty, including theft, plagiarism, disruptive conduct and misuse of materials and property, must guide your computing activities, just as they guide your activities in the classroom, residence halls or elsewhere on campus.

- Don't let other students, relatives or any other person gain access to the University's computing resources through your account. You will be held accountable for any abuse of computing resources by persons you allow to use your University computing accounts. Don’t use computing accounts or computing IDs and passwords that belong to someone else.

- Don't hide your identity to avoid responsibility for your behavior on the network or use someone else’s network identity.

- Know that local, state and federal laws and regulations apply to computing activities -- laws dealing with fraud, forgery, harassment, extortion, threats, copyright, sexually explicit content, among others. Violators may be prosecuted.

- Understand that your access to computing resources can be revoked. The University extends these resources to students who are trusted to make responsible use of them. If you violate that trust, you may lose access to these computing resources.

IV. E-mail: Etiquette and Privacy

You may expect that the content of the e-mail messages you exchange with others is confidential because the University does not inspect e-mail content. You should be aware, however, that e-mail messages are records that are subject to review with sufficient justification; they may be subject to legal investigation requests placed through proper channels. Courts have ruled that e-mail records can be subpoenaed in some cases and the University's judicial system may determine that e-mail or other files are evidence that may be reviewed as part of the process. Under these circumstances, the privacy of your e-mail is not guaranteed.

E-mail messages may be preserved as computer files on centrally-administered disks, so it is possible for people other than yourself to see them. In this sense, they are not private.

People often make mistakes in addressing their e-mail which put private messages in the mailbox of someone other than the intended recipient. If you are the recipient of such a message, common courtesy dictates that you either return the message to the sender with a brief note explaining its misdirection or that you delete the message.
The University has established a mass e-mail policy that limits the sending of large-scale e-mailings to critical information only. Sending a message to a large volume of recipients may slow down the e-mail system, cause disk quota problems for users, and negatively impact our network bandwidth. Contact the Help Desk for guidance in determining which messages are eligible for mass e-mail. The mass e-mail policy may be viewed at http://academic.scranton.edu/department/helpdesk/massemail.html.

Other Rules of Etiquette

• Remember, the e-mail messages you send become the possession of the receiver. They can easily be redistributed by recipients. When in doubt, double-check the addresses of your intended recipients.

• Do think before you send e-mail -- once sent, electronic mail messages usually cannot be kept from reaching their destinations. Think of e-mail as letters, not phone conversations.

• Realize that secure passwords provide good but not complete assurance of the privacy of your e-mail messages. When the confidentiality of a message is of the utmost importance, only a person-to-person conversation may be sufficiently secure.

• Your password may be guessed or “cracked” if you choose a common word, a friend’s or a pet’s name, your nickname, the name of your favorite team, or the name of a celebrity. Choose a password that combines letters, numbers and special characters (for example, $, #, &). Whether you use your University computing accounts or not, it is your responsibility to keep them secure. Don’t keep your password and computing username together. It is best to remember your password without writing it down. Don’t tell anyone what your password is. Change your password regularly.

• Delete messages that should not be preserved.

• Don’t send chain e-mail, even when it promises you or someone else fame and fortune. It is a waste of computing resources and a nuisance and often offends recipients.

• Don’t use University e-mail for commercial purposes.

• Realize that if you die while you are a member of the University community, your stored e-mail is a part of your estate that will be given to your heirs (usually your parents) if they request it.

V. Student Web Sites on University Systems

The University’s Web server, software, courses, and training sessions are in place to help you publish web pages.

Responsibility
You are expected to act responsibly when publishing web pages, just as you are with every use of computing resources at the University. You assume full legal and moral responsibility for the content of your web pages. You must abide by all local, state, and federal laws that pertain to communication and to publishing. This includes libel and copyright laws. Copyright law pertains to all published material, including cartoons, pictures, graphics, text, song lyrics, and sounds (including most MP3 and other files downloaded via file-sharing technologies).

**Commercial Activity / Fundraising and Advertising**

You may not use University web sites for non-academic, commercial activity. This includes but is not limited to running any sort of private business through a University web site unless it is an approved University project. You may not use University web sites for fund raising or advertising for commercial or non-commercial organizations, except for University-related organizations and University-related events and in accordance with policies governing these activities.

**Use of the University Name, Logo, or Seal**

You may not use the University name in your web pages in any way that implies University endorsement of other organizations, products, or services. You may not use the University logo or seal. Photos from the University's web sites may not be used or reproduced in any form.

**VI. Copyright Policy at the University of Scranton**

Most software available for use on computers at the University is protected by federal copyright laws. Educational institutions are not exempt from the laws covering copyrights. In addition, software is normally protected by a license agreement between the purchaser and the software seller. The software provided through the University for use by students may be used only on computing equipment as specified in the various software licenses.

It is the policy of the University to respect the copyright protections given to software owners by federal law. It is against University policy for students to copy or reproduce any licensed software on University computing equipment, except as expressly permitted by the software license. Also, you may not use unauthorized copies of software on University-owned computers or on personal computers housed in University facilities. Unauthorized use of software is regarded as a serious matter and any such use is without the consent of the University and subject to disciplinary action.

Unauthorized use of other copyrighted or licensed materials including, but not limited to, graphic images, music, video or audio files, and writings, is also regarded as a serious matter and is a violation of federal law. Because of the widespread availability of new file-sharing technologies, which make copyrighted materials freely and easily accessible without any payment to copyright holders, particular attention should be paid to this use of copyrighted creative works. The unauthorized use of copyrighted materials, including music, is both legally and ethically wrong. It is illegal in that it constitutes copyright infringement. Intellectual property, including music, is owned by someone other than the student user, and the owner may sue you if you use that property without permission or license. For more information on copyright and intellectual property, go to the U.S. Copyright Office web site at [http://lcweb.loc.gov/copyright/](http://lcweb.loc.gov/copyright/). It is unethical in that it directly takes income away from people who
make their living from these copyrighted materials and consequently, it erodes the integrity of the University.

VII. What You Should Do if You Are a Victim of Computer Abuse

Unfortunately, computer abuse, harassment, malicious behavior, spamming and unauthorized account access happen. Should any of these things happen to you, report them to the Help Desk. Complaints will be reported to the Director of Systems and Software Resources. If appropriate, the complaint will be referred to the CIO. The Computer Use Board (CUB) may review these complaints and recommend the appropriate referral. Retain any harassing e-mail messages, dates and times of unauthorized access, etc., for investigative purposes. If possible, leave the messages in your electronic mailbox.

VIII. Investigation Guidelines

Unauthorized use or any violation of this policy is subject to investigation and enforcement as outlined in guidelines below. Investigation may require the suspension of access to computer resources and inspection of files. Enforcement of this policy may lead to University disciplinary action, and/or prosecution under federal, state, and/or local laws. Investigations of suspected computer abuse shall be conducted with consideration of the duties and rights of all parties involved. These guidelines provide certain procedures to follow during an investigation. CUB will assist with the interpretation of the code but will not actively participate in the investigation.

A. Denial of Access to Computing Resources

A system administrator may deny access to computing resources in the following specific cases.

1. In cases where a system administrator may reasonably judge that a computing resource is in jeopardy due to the actions traced to a particular authorized user, that student's authorization may be immediately suspended.

2. In cases where a system administrator may reasonably judge that other users are being deprived of their legitimate use of the computing resource due to actions traced to a particular authorized user, that student's authorization may be immediately suspended.

3. In cases not covered by 1 and 2, where a system administrator may reasonably judge that a violation of the code is traced to a particular authorized user, the normal procedure shall be to attempt to contact the authorized user to set up a meeting to discuss the problem. If, after one week from the initial attempt to contact the user, the meeting has not taken place, that student's authorization may be suspended.

This denial of access may continue until the matter is resolved. However, an individual whose access has been denied has the right to meet with the system administrator at the earliest opportunity.

B. Inspection of Computer Information
During the course of an investigation of a suspected violation, it may be judged necessary to inspect information created, transmitted, or stored on University computer resources. Since this is a very sensitive issue which deserves careful consideration, files may be inspected only with the express consent of CUB and with at least one member of CUB present at the inspection. Furthermore, the user whose files are to be inspected must be given ample opportunity to be present at the time the files are inspected.

It should be made clear that the archiving of all files -- suspicious or not, without inspection, is normally done as a routine part of system maintenance and may be done as a routine part of investigation. Archived information may provide material for investigation. It is hoped that the actual inspection of files may be avoided except in extreme cases where it may be necessary.

Actions taken under guidelines A and B are not sanctions but a way of handling an immediate problem. They are taken to assure the quality of computing for the whole University community.

CUB shall consist of one person from the following constituencies who will serve two year terms.

1. Information Resources (appointed by the CIO)
2. Student body (appointed by the Vice President for Student Affairs)
3. Administration or non-IR Clerical/Professional staff (appointed by the Provost)
4. Faculty (appointed by the Faculty Senate)
5. The General Counsel

CUB shall elect its own chair.

CUB shall act as a third party observer/advocate where required or requested in investigations of suspected violations of the Student Computing Policy. A written report which specifies the procedures utilized in the investigation shall be submitted by CUB to the CIO at his/her request. CUB may recommend changes in the Student Computing Policy.

Computing offenses by students will be resolved by the appropriate system administrator, the CIO or within the University of Scranton judicial system. Students found culpable of violating this policy shall face penalties such as the loss of computing privileges, warnings, fines, participation in community service work, residential or disciplinary probation, residential eviction, required residence in University approved housing as a condition of continued enrollment, suspension or expulsion.

Non-students having no affiliation with the University and who have violated these regulations shall be referred to the relevant civil and/or criminal authorities for appropriate action.