Code of Responsible Computing for Faculty & Staff

The following University of Scranton code addresses the responsible use of information and technology resources, violations of policy, and guidelines for effective use of technology resources. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. These policies and guidelines are subject to change as state and federal laws develop and change. Suggestions on these policies are welcomed and should be sent to the CIO at planning@scranton.edu.

Contents:

1. Individuals Covered
2. The University of Scranton's Policy on Responsible Computing
3. Computing Violations
4. Copyright and Trademark at the University of Scranton
5. E-mail Guidelines: Privacy and Etiquette
6. University Technology Resources: Ownership
7. Computer Viruses
8. What You Should Do if You Are a Victim of Computer Abuse
9. Investigation Guidelines

Individuals Covered

This policy applies to all non-students accessing The University of Scranton’s computing and network facilities. These persons include faculty, staff, persons retained to perform University work, and any other persons extended access and use privileges by The University

The University of Scranton's Policy on Responsible Computing

All individuals covered under this policy have the responsibility to use University computing and network facilities in an ethical, professional, and legal manner as well as in accordance with The University’s mission. Civil discourse is at the heart of a University free from intimidation and harassment and based upon a respect for individuals and a desire to learn from others. While debate on controversial issues is inevitable and essential, bear in mind that it is everyone’s responsibility to do so in a way that advances the cause of learning and mutual understanding. This policy supports the principles of academic freedom.

This means that users agree to abide by the following conditions:

- Use the University’s computing facilities and information resources, including hardware, software, networks, and computer accounts, responsibly and appropriately. Respect the rights of other computing users, and respect all contractual and licensing agreements.
- Do not use computers or computer accounts which require authorization unless such has been granted to you.
• The University's network and computer infrastructure is a finite resource. Use computer accounts for the purpose(s) for which they have been issued. Commercial use of the University's computing resources, not related to approved University projects is prohibited.
• Be responsible for all computer accounts and for protecting each account's password.
• Report unauthorized use or abuse of your accounts to your supervisor, system administrator, or other appropriate University authority.
• During an investigation of a problem, cooperate with Information Resources' requests for information about computing activities.

Computing Violations

• Examples of prohibited actions that are subject to disciplinary review include:
• Attacking the security of the system or failing to maintain the security of the system;
• Using obscene or abusive language in electronic communications;
• Using any computing resources to intimidate, insult or harass others; to interfere with an individual’s work or educational performance; or to create an intimidating, hostile or offensive working/learning environment;
• Accessing or attempting to access another individual's data or information without proper authorization;
• Tapping phone or network lines;
• Use of network sniffers without authorization;
• Intentional release of a virus, worm, or other program that damages or harms a system or network;
• Preventing others from accessing services;
• Modifying, divulging, damaging or destroying confidential information without authorization;
• Downloading or posting to university computers, or transporting across the university networks, material that is unlawful, proprietary, or in violation of university contracts.
• Malicious use of computing resources to damage the institution.
• Use of computing resources for partisan political objectives and/or campaign (not including the expression of personal political views, scholarly dialogue, or debate).
• Use of computing resources other than bboard for solicitation.
• Violations of federal, state, or local laws.

Copyright and Trademark 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 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 persons covered by this agreement 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. Any unauthorized use of software without the consent of the University will subject the user 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 regarded as a serious matter and is a violation of federal law. The unauthorized use of copyrighted materials is unlawful copyright infringement. For more information on copyright, go to the U.S. Copyright Office web site at http://lcweb.loc.gov/copyright/.

Use of University trademarks, service marks, or logos, including but not limited to the wordmark found on University letterhead and the seal, not in connection with University business is not permissible. Unauthorized use of trademarks, service marks or logos of other entities in connection with use of University computing and network facilities is also prohibited.

**E-mail Guidelines: Privacy and Etiquette**

Faculty and staff can expect that e-mail messages are treated confidentially because the University does not monitor employees' e-mail transactions. However, e-mail messages are written records that could be subject to inspection under Section IX, Investigation guidelines. Courts have also ruled that e-mail records and information in electronic form can be subpoenaed in some cases. The University does not guarantee the privacy of e-mail.

When system problems occur, such as hardware or software failure or attacks by malicious users, the staff who maintain the e-mail servers are authorized to look at any information and any files on university computers that are necessary to solve the problems and to protect the systems and the information they contain. It is part of the system administrator's job to do this and to treat any information on the systems as confidential.

In addition to the authorized actions of system administrators, e-mail can end up in the hands of computing staff if it was inaccurately addressed and if it could not be delivered. People also make small mistakes in addressing their e-mail so that private messages appear in the e-mailbox of someone other than the intended recipient.

**E-mail guidelines:**

- E-mail is not always from the person who is specified on the From line. It is relatively easy to impersonate a user when sending e-mail. Be wary of messages with questionable content.
• Just like written letters, the e-mail messages are owned by the receiver. They can easily be redistributed or copied by the recipients.
• Realize that University policy and secure passwords provide good but not complete assurance of the privacy of e-mail messages. When the confidentiality of a message is of the utmost importance, only a person-to-person conversation may be sufficiently secure.
• Delete messages that should not be preserved.
• Chain e-mail, a message that requests that you forward it to others, should not be forwarded.

**University Technology Resources: Ownership**

The University owns the servers, departmental computer labs, 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 servers, computer labs, and office 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. The University will make every effort to secure and maintain the integrity and functionality of all available network resources.

While the University of Scranton owns the computers in all the offices and departments, each individual staff or faculty member makes the decision about how that equipment will be used. The University also owns the software licenses (word processing, spreadsheet software, e-mail, etc.) that were purchased from a software vendor using university funds. The licenses usually allow for the installation of one copy of the software.

With the proliferation of Wireless technology, the university asserts ownership to campus air space for the purposes of providing a centrally managed wireless network infrastructure.

**Computer Viruses**

Computer viruses are programs that interfere with the running of normal programs. Some viruses are more of a nuisance than an actual cause of damage to the computer system or data. Other viruses, however, destroy data and render computer systems inoperable. Any person knowingly promulgating a virus in any format is subject to disciplinary action by the University.

Computer virus guidelines:

• Freeware and shareware can be very hazardous to University computing resources. Be wary of downloading files from non-University sources.
• Back up important files at least weekly. Routinely check backup copies. Keep multiple backup copies.
• Use anti-virus software.

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, where the appropriate action will be initiated. If appropriate, 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 any evidence on your computer system.

Investigation Guidelines

The primary responsibilities of Information Resources are neither investigative nor disciplinary. However, in cases where University resources and privileges are abused or otherwise threatened, the staff will take appropriate steps 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.

1. Denial of Access to Computing Resources

A system administrator may deny access to computing resources in the following 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 user'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 user'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 user'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 and his or her supervisor.
2. 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 an opportunity to be present at the time the files are inspected.

It should be made clear that the archiving of all files on University servers is normally done as a routine part of system maintenance and may be done as part of an investigation. 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.

3. Computer Use Board

CUB shall act as a third party observer/advocate where required or requested in investigations of suspected violations of this policy. CUB may recommend changes in this policy. CUB shall consist of one person from the following constituencies who will serve two-year terms.

1. Information Resources (appointed by the CIO)
2. Human Resources (appointed by the Director of Human Resources)
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.

A written report which specifies the procedures utilized in the investigation shall be submitted by CUB to the CIO, who will determine whether this policy has been violated.

Computing violations by faculty will be resolved by existing procedures and practices. Computing violations by staff will be resolved by the appropriate supervisor in consultation with Human Resources based upon the Employee Handbook.

Any user having no affiliation with The University and who has violated these regulations in the judgment of appropriate University personnel shall be denied computing privileges and may be referred to the relevant civil and/or criminal authorities for appropriate action.