Acceptable Use of Information Technology Resources

The primary references for this document can be found at:

http://www.policy.umn.edu/Policies/it/index.htm

http://www.policy.umn.edu/Policies/it/Use/ITRESOURCES.html

Policy Statement

Computers, networks and electronic information systems are essential resources for accomplishing the University of Minnesota's mission of instruction, research, and service outreach. The University grants members of the University community shared access to these resources in support of accomplishing the University's mission.

These resources are a valuable community asset to be used and managed responsibly to ensure their integrity, security, and availability for appropriate educational and business activities. All authorized users of these resources are required to use them in an effective, efficient, and responsible manner.

Users must be aware of User Rights and Responsibilities, which outline liability for personal communication, privacy and security issues, and consequences of violations. Users should also be aware of the University's Rights and Responsibilities, as well as any additional requirements of their individual unit or campus.

Reason for Policy

The purpose of this policy is:
- to safeguard the integrity of computers, networks, and data, either at the University of Minnesota or elsewhere;
- to ensure that use of electronic communications complies with University policies;
- to protect the University against damaging legal consequence

User's Rights and Responsibilities

Members of the University community are granted access to information technology resources in order to facilitate their University-related academic, research, and job activities. The Regents Policy on Academic Freedom extends to information resources that are available electronically. However, by using these resources, users agree to abide by all relevant University of Minnesota policies and procedures, as well as all current federal, state, and local laws. These include but are not limited to University policies and procedures related to harassment, plagiarism, commercial use, security, and unethical conduct, and laws prohibiting theft, copyright and licensing infringement, unlawful intrusions, and data privacy laws.

Users are responsible for:
- reviewing, understanding, and complying with all policies, procedures and laws related to access, acceptable use, and security of University information technology resources;
- asking systems administrators or data custodians for clarification on access and acceptable use issues not specifically addressed in University policies, rules, standards, guidelines, and procedures; and
- reporting possible policy violations to the appropriate entities listed in this document (in the Contacts and Procedures sections).

Liability for Personal Communications

Users of University information technology resources are responsible for the content of their personal communications. The University accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

Privacy and Security Awareness

Users should be aware that although the University takes reasonable security measures to protect the security of its computing resources and accounts assigned to individuals, the University does not guarantee absolute security and privacy. Users should follow the appropriate security procedures listed in the Using Information Technology Resources Standards (Appendix A) to assist in keeping systems and accounts secure.

The University assigns responsibility for protecting its resources and data to system administrators and data custodians, who treat the contents of individually assigned accounts and personal communications as private and does not examine or disclose the contents except:

- as required for system maintenance including security measures;
- when there exists reason to believe an individual is violating the law or University policy; and/or
- as permitted by applicable policy or law.

Consequences of Violations

Access privileges to the University's information technology resources will not be denied without cause. If in the course of an investigation, it appears necessary to protect the integrity, security, or continued operation of its computers and networks or to protect itself from liability, the University may temporarily deny access to those resources. Alleged policy violations will be referred to appropriate University investigative and disciplinary units. For example, alleged violations by students may be directed to the Student Judicial Affairs office. The University may also refer suspected violations of law to appropriate law enforcement agencies. Depending on the nature and severity of the offense, policy violations may result in loss of access privileges, University disciplinary action, and/or criminal prosecution.

Medical School Duluth Campus Policy References and Supplemental Links

Rules for Computer Lab Use

I. Computer use in SMED 68 is limited to administration of exams. Any other use, unless specifically authorized, is not allowed, including email and web use.
II. The Medical School Duluth Campus will make every effort to provide computer services to meet the student and coursework demands. Excess amounts of printing will be monitored and addressed as needed.
III. Absolutely no software piracy will be tolerated. Any student caught copying copyrighted software or illegally using or distributing copyrighted software will immediately have their access to the computer lab areas revoked and will be referred to the Medical School Duluth Campus Honor Council.
IV. Absolutely no physical abuse of equipment, software, or data will be tolerated.
V. Absolutely no misuse of central systems, the network, or other systems on the network will be tolerated. This includes, but is not limited to: breaking into, halting, slowing down, or breaking security of the network or systems on the network (or efforts or attempts at doing these things); abusing another person's data or account; harassment or abuse of other users on the network or systems on the network.

Consequences for Breaking Academic Computer Use Rules

The consequences for breaking any of the above rules will depend on the seriousness of the offense. Serious offenses will be referred to the Medical School Duluth Campus Honor Council. In most cases the following series of events will occur:

1. The person will be contacted by a staff person at the first possible opportunity. When the problem is class-related the instructor of the course involved will also be contacted.
2. If an agreement cannot be reached at that time, or the person cannot be reached, computing access will be revoked until an agreement is reached.
3. If discussions cannot be initiated or agreement cannot be reached, the problem will be immediately referred to the Medical School Duluth Campus Honor Council and/or presented to the University of Minnesota Duluth Student Conduct Code Coordinator..
4. A hold may be placed on a student's records if there are outstanding charges for damaged equipment or for other cost recovery related items.
5. As required, the incident will be referred to the criminal authorities for violations of city, state and/or federal laws.

Security Policies

In order to ensure appropriate use of computer hardware, software, and networks, systems are monitored and when observed, unusual activity is investigated by system administrators. The use of wireless networks at the University of Minnesota Medical School Duluth Campus require all connecting devices be authorized and secured. Additionally, any computer connecting to network services of the University of Minnesota must comply with all standards and security policies. The most recent changes are highlighted below:

Virtual Private Network
http://www.d.umn.edu/itss/vpn/

OIT Security
http://www.oit.umn.edu/safe-computing/personal-computer/

Protecting Private Data Standard
http://www.oit.umn.edu/security/topics/managing-data/

Secure Data Deletion Standard
http://www.oit.umn.edu/security/topics/data-deletion/

Changes and updates to policies will be regularly posted to the websites of the University of Minnesota.

Appendix A: Using Information Technology Resources Standards
(http://www.policy.umn.edu/Policies/it/Use/ITRESOURCES_APPA.html)

Use of IDs and Passwords

- Do not share the account name or password assigned to you.
- Select an obscure password and change it frequently.
- Understand that you are responsible for all activities on your username/account ID.
- Ensure that others cannot learn your username/account ID or password.
- If you have reason to believe that your username/account ID or password has been compromised, contact your System/Network Administrator immediately.

Use of Information/Data

- Access only accounts, files, and data that are your own, that are publicly available, or to which you have been given authorized access. Secure information that is in your possession.
- Maintain the confidentiality of information classified as private, confidential or data on decedents.
- Use University information for tasks related to job responsibilities and not for personal purposes.
- Never disclose information to which you have access, but for which you do not have ownership, authority, or permission to disclose. Keep your personal information/data current.
- Accurately update your own records through University self-service systems and other processes provided for you.

Use of Software and Hardware

Use University e-mail, computers, and networks only for legal, authorized purposes. Unauthorized or illegal uses include but are not limited to:
- Harassment;
- Destruction of or damage to equipment, software, or data belonging to others;
- Unauthorized copying of copyrighted materials; or
- Conducting private business unrelated to University activities.

Never engage in any activity that might be harmful to systems or to any information/data stored thereon, such as:
- Creating or propagating viruses;
- Disrupting services or damaging files; or
- Making unauthorized or non-approved changes.

Social and Online Media Participation Guidelines

The Academic Health Center is preparing guidelines to serve as best practices for Medical School faculty, staff, students, and affiliated residents and fellows who participate in blogging, social networking sites and other social media. While the guidelines are not ready for distribution, please keep in mind that you have a responsibility to present yourself and represent the University in a professional manner. The Medical School Duluth Campus Honor Code and the Medical Student Professionalism Code provide guidance, as do these existing policies:

University of Minnesota Duluth Guidelines on Social Networking
http://www.d.umn.edu/itss/policies/socialnetwork.html

Social networking information
http://www.webdepot.umn.edu/social_guidelines.php

Administrative policy
http://policy.umn.edu/Policies/it/Use/ITRESOURCES.html