

4.0 Acceptable Use Policy

4.1.0 Purpose

It is the intent of Upper Iowa University to provide a quality technological environment for the University community in which certain standards are observed. Computers, computer systems and other electronic equipment are the property of UIU. Use of University technology resources is a privilege and not a right. Therefore, use of such resources is contingent upon compliance with University policies and standards and all governing federal, state and local laws and regulations.

4.2.0 Scope

This policy applies to all users of information technology within the University.

4.3.0 Policy

4.3.1 Acceptable uses of technology resources

The purpose of Upper Iowa University's informational technology resources is to support education, research and communication. The following are acceptable uses of Upper Iowa University's information technology resources (environment):

1. Class assignments
2. Academic research and investigation
3. Computing for personal and professional advancement
4. Administrative and instructional support
5. Staff and faculty consulting (subject to provisions contained in relevant personnel policy)
6. Personal use by permitted users that does not disrupt, interrupt or diminish access to resources for other users and does not violate any applicable law, regulation or University policy

Use of Upper Iowa University computing facilities is restricted to current employees and students, to ensure compliance with acceptable use policies of the Internet and to maintain the security of administrative computing systems. All users are required to obtain permission to access the University's administrative system through their own personal or laptop computer. All users who are given access must have an anti-virus and anti-spyware package installed with the current updates applied on the computer. (See form 101) System resources such as network servers, processor performance, and disk space are routinely monitored by Information Technology personnel to ensure system security and integrity. Anyone using shared computing facilities at Upper Iowa University implicitly consents to such monitoring by authorized personnel.

4.3.2 Unacceptable uses of technology resources

The Upper Iowa University campus network includes campus-based computer systems, wide-area networks (WANs), local-area networks (LANs), telecommunications equipment, and the high-speed network linking the campus to the worldwide Internet. Upper Iowa University computer users must not engage in unauthorized or inappropriate conduct on the Internet or Upper Iowa University WAN/LAN networks or facilities.

Examples of such inappropriate activities include:

1. Using or sharing another person's log-in ID to access computing facilities at Upper Iowa University or another Internet facility. This includes permitting others to use your own log-in ID.
2. Using Upper Iowa University facilities to crack or access systems, whether on campus or off, in an unauthorized or inappropriate manner.
3. Using Upper Iowa University networking facilities to engage in illegal or criminal activities.
4. Using Upper Iowa University networking facilities to threaten or harass another person.
5. Downloading or installing software on a University computer unless Information Technology specifically designates and authorizes them to do so. (See form 102)
6. Attempting to read or access another person's electronic mail or other protected files.
7. Copying or distributing software that violates copyright laws, license agreements, and intellectual property, as outlined in the Copyright Law of the United States of America, revised March 1, 1989, in Title 17 of the United States Code, Section 117, including unauthorized peer-to-peer file sharing and illegal downloading of copyrighted material that includes but not limited to music, video, software and eBooks.
8. Knowingly distributing or actively developing a computer virus, worm, or Trojan horse.
9. Repeated use of Upper Iowa University networked facilities in a discourteous manner, including: using excessive amounts of system resources (e.g., CPU time, band width or disk space), thereby preventing access by other users; consuming excessive volumes of printing resources; sending unwelcome electronic mail messages and posting information to public folders that is inappropriate; disturbing others while using public-access computing laboratories; participation in chat groups that are not specifically required by job; refusing to yield workstations in public labs to users for activities of higher priority.

Computer resources have been allocated for World Wide Web activities that support research, education, administrative processes, and other legitimate pursuits. All activities must be consistent with this purpose. Violations include, but are not limited to:

1. Emailing commercial activities that are not approved by University administration
2. Creating, displaying, or transmitting threatening, racist, sexist, obscene, or harassing language and/or materials
3. Violation of personal privacy

4. Vandalism and mischief that incapacitates, compromises, or destroys University resources and/or violates federal and/or state laws
5. Commercial advertising; displaying pornography or racist jokes
6. Posting private personal information without permission such as grades, medical records, or any other information that is protected by the Public Records Law
7. Providing information or instructions to compromise University security measures

4.3.3 Email Policy

System administrators are expected to treat the contents of electronic files as private and confidential. Inspection of electronic files and electronic mail, and any action based upon such inspection, will be governed by all applicable federal, state and local laws. The Upper Iowa University community is advised that all files stored on main systems, including electronic mail, are backed up regularly and may be subject to subpoena.

4.3.4 ISP Acceptable Use Policy

Upper Iowa adheres to the acceptable use policies of our internet service providers.

4.3.5 Use of Personal Web Pages

Personal Web pages are permitted for University faculty, staff and student organizations (student organizations must be in good standing with the University). Personal Web pages for individual students are permitted only when assigned as a class project.

Personal Web pages must adhere to all sections of this Acceptable Use of Technology policy. Authorization to post personal Web pages must be obtained through the Director of Web Services and the Director of Information Technology. (See form 103)

Because these pages are personal and not part of the University's official Web site, Web Services or the Information Technology Team will not provide any Web page creation or design services.

4.3.6 University website

Refer to Marketing & Communications website [policies](#).

4.3.7 Sanctions Procedures

Suspected violations of the Computer Use Policy are to be reported in writing to the Director of Information Technology. The Director will be responsible for the investigation of the alleged violation. Based on the findings the Director will have the right to temporarily suspend the computer privileges of the individuals involved in the violation until the completion of the University judicial process. As a part of the investigation it may become necessary for college authorities to examine electronic files, accounting information, printouts, tapes, or any other materials on University equipment. For potential liability reasons, the University reserves the right to monitor all communications on the University's system.

The Director of Information Technology will forward the findings of the investigation to the appropriate University official for further disciplinary action as follows: for student violations, the Dean of Student Development or the Center Director, Program or Regional Director; for faculty violations, the Dean of Faculty for the Fayette campus or the AVP of Academic Extension; or for staff violations, the direct supervisor. The appropriate University official will follow the disciplinary hearing procedures as outlined in the Student Handbook.

Sanctions for the violations of the Computer Use Policy may include but are not limited to loss of computer privileges, reprimand, suspension or expulsion for students and discharge from employment to possible prosecution by state and federal authorities for employees.

4.3.8 Disclaimer

Upper Iowa University does not warrant that the functions or services performed by or that the information or software contained on the University's technology resources will be kept confidential, meet the user's requirements or that resources will be uninterrupted or error-free or that defects will be corrected. The University does not make any warranties, whether expressed or implied including, without limitation, those of merchantability and fitness for a particular purpose, with respect to any technological products or services or any information or software contained therein.

4.4.0 Revision History

Date	Revision #	Description of Change

4.5.0 Inquiries

Terry Smid
Director of IT
Upper Iowa University
Email: smidt@uiu.edu