INFORMATION TECHNOLOGY POLICY

NUMBER/TITLE: 500 / Acceptable Use of Technology

Covered Individuals: All stakeholders
Covered Locations: All locations
Effective Date: 11/2009
Strategic Priority: SP
HLC: Criterion
Consultations:

POLICY STATEMENT

Appropriate organizational use of information and information technology ("IT") resources and adequate security of those resources require the participation and support of the organization's users. Inappropriate use exposes the university to potential risks, including virus attacks, compromise of network systems and services, and legal issues.

PURPOSE

This policy is designed to establish the acceptable and appropriate use of all information technology resources that support the mission of Upper Iowa University (University or UIU). Use of such resources is contingent upon compliance with university policies and standards and all governing federal, state and local laws and regulations.

DEFINITIONS

University Technology – desktop and laptop computer hardware and software; core technology such as data networks, storage, servers, and communication infrastructure systems; University/department-wide software and cloud services; and any contractual technology services.

Organization – Upper Iowa University (UIU)

POLICY IMPLEMENTATION

The purpose of UIU's information technology resources is to support education, research and communication. The following are acceptable uses of the 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 handbook and/or 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 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. Periodic monitoring of system resources such as network servers, processor performance, disk space, and forms of electronic communication (including email, text messaging, instant messaging, and other electronic records), are conducted by the Information Technology Services departmental personnel to ensure system security and integrity. Anyone using shared computing facilities at the University implicitly consents to such monitoring by authorized personnel.

In addition to the notice provided in this policy, users may be notified with a warning banner text at system entry points where users initially sign on about being monitored and may be reminded that unauthorized use of the organization's IT resources is not permissible.

Unacceptable uses of technology resources
University users must not engage in unauthorized or inappropriate conduct when utilizing University technology resources.

1. Unacceptable use includes, but is not limited to, the following: Using or sharing another person's log-in ID to access computing facilities at UIU or another Internet facility. This includes permitting others to use one's own log-in ID.
2. Using University facilities to crack or access systems, whether on campus or off, in an unauthorized or inappropriate manner.
3. Using University networking facilities to engage in illegal or criminal activities.
4. Using 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 it.
6. Attempting to read or access another person's email or other protected files.
7. Copying or distributing software that violates license agreements or copyright law, as stated in U.S. Copyright Law, in Title 17 of the U.S. Code, Section 117, including unauthorized peer-to-peer file sharing and illegal downloading of copyrighted material that includes but is 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 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 email messages and posting information to public folders that is inappropriate; disturbing others while using public-access computing labs; participation in chat groups that are not specifically required by the job; refusing to yield workstations in public labs to users doing work of higher priority.

Technology resources have been allocated for 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 public records law.
7. Providing information or instructions to compromise University security measures.

Artificial Intelligence
You may not enter sensitive, restricted, or otherwise protected data into any generative AI tool or service. This information includes, but is not limited to:

- FERPA-protected or regulated information, such as:
    - Organization Name IDs or photos

    - Organization Name Directory data
    - University non-directory data such as student ID numbers
    - Work produced by students to satisfy course requirements
    - Student names and grades
    - Disability-related information
- Health information protected by HIPAA
- Information related to employees and their performance
- Intellectual property not publicly available
- Material under confidential review, including research papers and funding proposals
    - For further academic information regarding AI reference: https://uiu.edu/wp-content/uploads/PC-AA-152_Generative-AI-Use-clean-copy.pdf
- Information subject to export control

Protecting sensitive information and complying with applicable state and federal privacy and security laws and regulations and with institutional policies is imperative.
Access to protected institutional data must be authorized and managed to protect individual privacy, maintain promised confidentiality, and ensure appropriate access and use.
You may not upload any data that could be used to help create or carry out malware, spam, phishing, or other scams. System IT resources may not be used to disseminate unauthorized email messages.
You may not direct AI tools or services to generate or enable content that facilitates sexual harassment, stalking, or sexual exploitation or that enables harassment, threats, defamation, hostile environments, stalking, or illegal discrimination, including, but not limited to:

- Sexual harassment, stalking, dating violence, and domestic violence.
- Depicting a person's voice or likeness without their consent or other appropriate rights, including unauthorized impersonation and non-consensual sexual imagery.
- Harming or abuse of a minor, including grooming and child sexual exploitation.
- Harassing, harming, or encouraging the harm of individuals or specific groups, including discrimination or harassment based on a protected class.
- Discrimination based on disability or defects.

You may not use AI tools or services to generate content that helps others break federal, state, or local laws, institutional policies, rules, guidelines, licensing agreements, or contracts. System IT resources may not be used to violate laws, policies, or contracts.
You may not use AI tools or services to infringe copyright or other intellectual property rights.
You may not use, facilitate, or allow others to use artificial intelligence for:

- Intentional disinformation or deception.
- Violating the privacy rights of others, including unlawful tracking, monitoring, and identification.
- Intentionally circumventing safety filters and functionality or prompting models to act in a manner that violates UIU's Policies.
- Performing a lethal function in a weapon without human authorization or control.

User Responsibility for IT Equipment
Users are routinely assigned or given access to IT equipment in connection with their official duties. This equipment belongs to the organization and must be immediately returned upon request or when an employee is separated. Users may be financially responsible for the value of equipment assigned to their care if it is not returned to the organization.
Should IT equipment be lost, stolen, or destroyed, users must provide a written report of the incident's circumstances. Users may be subject to disciplinary action, which may include repayment of the replacement value of the equipment. The organization will not issue or re-issue IT devices and equipment to users who repeatedly lose or damage IT equipment.

Sanctions for the violations of this policy may include, but are not limited to, loss of computer privileges,

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

CUSTODIAN

Acting as the Policy Owner, the Executive Director of Information Technology Services (ED of ITS) is responsible for answering questions regarding the application of this policy.

RELATED DOCUMENTS, FORMS, AND POLICIES

502 Email Use Policy
https://uiu.edu/wp-content/uploads/502-Email-Policy.pdf

505 Website Privacy Policy
https://uiu.edu/wp-content/uploads/505-Website-Privacy-Policy-6-Mar-2019-1.pdf

AA-152 Generative AI Use
https://uiu.edu/wp-content/uploads/PC-AA-152_Generative-AI-Use-clean-copy.pdf

HISTORY

New/Revision Number	Date of Action/Approval	Revision Change
	11/2009	New
	May 11, 2020	Revised policy considered by University Policy Committee (UPC); vote put on hold until additional changes are made.
	May 14, 2020	UPC electronic vote in favor of policy draft as amended; policy recommended to President's Council (PC).
	May 20, 2020	PC makes some edits, recommends approval to President Duffy, the President approves policy.
	July 9, 2025	PC makes edits, recommends approval to President Franken.