Computer Usage Policy

Introduction

The University provides an opportunity for students and other members of the UAM community to enhance their educational experiences and expand their academic knowledge by making available to them access to computer facilities and resources, including the Internet. This technology places a significant amount of information and responsibility in the hands of its users. This policy has been created to define what the University of Arkansas at Monticello considers responsible and ethical behavior in using its computing facilities and resources and is applicable to all UAM faculty, staff, students, and guests.

Our Computer Usage Policy supports UASP 285.1 and UAM OP 250.6. Any violation of UASP 285.1 or the University policy on using technology resources shall be subject to the progressive discipline policy. Depending on the severity of the violation, disciplinary action may include suspension or termination.

Computing activities and products must be compatible with UAM's Computer Usage Policy as well as federal and state statutes. Engaging in any activity which violates the Computer Usage Policy can result in the immediate suspension of an individual's computer access. Other penalties may include disciplinary action by UAM and/or legal action. Anyone who has questions about the acceptability of a contemplated use of computing resources should call the Department of Information Technology at 870-460-1036.

Purpose of Computing and Networking Resources

Computing and networking resources have been allocated for academic activities that are consistent with the mission and goals of the University, i.e., to support teaching, research, administrative processes, UAM-sponsored community service, and other legitimate pursuits. Each faculty and staff member are eligible for an email account, as is any student who has been officially admitted.

Administration

The UAM Department of Information Technology is responsible for administering the campus network to include all computer resources. While Information Technology has authority to enforce the Computer Usage Policy, it seeks to place its efforts toward the enhancement of technology resources, not the policing of these resources. Responsibility is placed on individual users to utilize campus computing resources in an effective, efficient, ethical, and lawful manner.

Disclaimer

The University recognizes the value and potential of electronic communications and publishing on the Internet (ex: emails, blogs, webpages, and social media posts). The University accepts no responsibility for the contents of web pages or electronic communications produced by students, faculty, or staff outside of the official UAM website and approved social media accounts. Views and opinions expressed in e-mail and electronic forums are strictly those of the authors.

Privacy of Electronic Files,

The right to privacy of electronic mail and other electronic files against unwarranted or unreasonable entry or search is a basic tenet of university policies. Authorized University officials will access or enter electronic files (including e-mail files) only under one or more of the following conditions:

- The user requests or gives permission to the University to access his/her account.
- There is a valid search warrant or court order.
- There exists an emergency in which the physical safety and/or well-being of a person(s) may be affected, or University property may be damaged or destroyed. Responsibility for authorizing access lies with the CIO or the Vice Chancellor for Finance and Administration, or the Chancellor
- Reasonable grounds exist to suspect a violation of law or University policy is occurring. Responsibility for authorizing access lies with the CIO or the Vice Chancellor for Finance and Administration.
- Personnel authorized by the CIO, or the Vice Chancellor for Finance and Administration must access the files to maintain the integrity of the computer system or to protect the rights or property of the University.

Proper Authorization

Use of UAM systems is restricted to authorized faculty, staff, alumni, and students. The administrator of a campus system, server, and/or campus network component is the responsible authority, which grants authorization for system use and access. Authorization forms are required for access to specific data and must be signed by a Vice Chancellor.

Official Electronic Communications

Student email accounts are created when applications are received and faculty/staff emails accounts are created when an authorization form is completed. UAM email is the official means of electronic communication with students, faculty, and staff. Important university information will be sent to individual email accounts.

University Email System

UAM email accounts should not be used:

- To send unauthorized mass mailings of any type.
- To send rude, obscene, harassing, or illegal material, or material that in any way conflicts with the regulations of the university.
- To send any material that in any way conflicts with state and federal law.
- To perform an operation or activity that degrades the performance of any system and/or network.

From UASP 285.1 referenced above:

No technology resources across the University are used to express a personal political opinion to an elected official unless the opinion is within the scope of the employee's regular job duties or the opinion is requested by an elected official or public entity; to engage in lobbying an elected

official on a personal opinion if the employee is not a registered lobbyist for the campus; to engage in illegal activities or activities otherwise prohibited by federal law or state law; or to intentionally override or avoid the security and system integrity procedures of the campus. Additionally, any political communication must be consistent with Board of Trustees Policy 465.1 and UA System Policy 465.1.

Copyright

Users must observe intellectual property rights including copyright laws as they apply to software, licensing, and electronic forms of information.

Violations

Computing and telecommunications resources may be used only for legal purposes and may not be used for any purpose which is illegal, unethical, dishonest, damaging to the reputation of the University, inconsistent with the mission and goals of the University, or likely to subject the University to liability. Impermissible uses (some of which may also constitute illegal uses) include, but are not limited to, the following:

- Unauthorized use of the account of another. The individual account owner is responsible for the proper use of the account, including proper password protection. Non-university affiliated individuals cannot be given access to computer accounts.
- Commercial or profit-making activities unrelated to the mission of the University or to University life.
- Unauthorized copying of any software which is licensed or protected by copyright.
- Failure to observe software copyrights and/or license agreements.
- Unauthorized copying or use of the intellectual work and property of others.
- Extensive use of the Internet for private or personal business.
- Unauthorized access to any University computer system and/or any computer system on
- the Internet.
- Creating, displaying, or transmitting threatening or harassing language and/or materials.
- Displaying obscene, lewd, or sexually harassing images or text that can be in view of
- others in a public facility or location.
- Misrepresentation of one's identity in electronic communications.
- Vandalism and mischief that incapacitates, compromises, or destroys University resources and/or security measures and/or violates applicable laws.

Hierarchy of Needs

Academic computing resources are provided in part so that users can learn, explore, and grow. However, activities related to the University's scholarly mission, such as completing class assignments or conducting research, take precedence over computing pursuits of a more recreational nature, such as exploring the Web or game playing. Game playing is specifically restricted to those times when resources are not needed for other purposes.
Authorized University personnel may ask recreational users to relinquish computer use to accommodate educational needs.

Enforcement

Minor infractions of this policy are resolved informally by Information Technology personnel. This may be done through electronic mail or in-person discussion and education. Examples of minor infractions are consuming excessive resources or overloading computer systems.

Repeated minor infractions or misconduct which is more serious may result in the temporary or permanent loss of campus computer or network access. More serious violations include, but are not limited to, unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior. The CIO or his/her designee has the authority to limit access based on the seriousness of the infraction.

Decisions limiting access to any faculty or staff member may be appealed through the normal grievance process as stipulated in the Faculty Handbook or Staff Handbook, respectively. Decisions limiting access to any student may be appealed through the Academic Appeals Process as stipulated in the Student Handbook.

Anyone who feels that a student has violated the UAM student conduct code using computing resources and/or facilities should contact the Associate Vice Chancellor for Student Engagement & Dean of Students to file a complaint against the offending party.

Updates

This policy is subject to change at any time. Occasional review is recommended.

Effective: April 1989

Updated: November 2023