



## Policy 01:010 – Use of Information Resources

The University of Montevallo has a significant investment in information technology resources and as owner of these resources has a responsibility to ensure the appropriate and lawful use of these resources. The purpose of this policy is to explain the guidelines that have been developed to ensure effective and appropriate use of Information Services and Technology (IS&T) resources and network services.

Access to the University of Montevallo's Information Services and Technology (IS&T) resources is a privilege, not a right. Information resources include, but are not limited to, computer hardware; software; mainframe resources; local area networks; access to external networks for local, national, and international sources of electronically generated, stored and transmitted information; University e-mail addresses; address lists and/or labels for faculty, staff, students, alumni and affiliates; and campus directories for faculty, staff, and students. Computers, communications equipment, and communications and computing networks are to be used by University of Montevallo students, faculty and staff for the sole purpose of facilitating and supporting the University's mission and administrative functions. It is the responsibility of each individual to ensure use of University IS&T resources in an appropriate manner and to comply with any Federal, State, or local statutes as they apply to IS&T resources. (See [Federal Communications Commission Rules & Regulations Title 47](#)).

Violations of policy or law may result in temporary or permanent loss of technology-related privileges, University sanctions, discipline up to and including immediate termination of employment, expulsion as a student, and/or other legal action.

### **Use of the Network**

The University of Montevallo's computing and network resources are to facilitate and support the mission of the University. Access is granted to the computing system and the network because it is a tool to meet the academic goals and the mission of the University.

University of Montevallo technology resources may not be used to create web pages for personal business or gain.

Advertising, selling, and/or soliciting by businesses, agencies or individuals are prohibited. Exceptions, if any, must be approved in writing by the vice president for the appropriate division and the Vice President of Business Affairs/Treasurer.

Use of a shared system and network carries certain obligations. All users shall assume full responsibility – legal, financial, or otherwise – for their actions on the network.

Web pages that are accessed to an excessive degree can be a drain on computer resources. Except where significant to the University's mission, such activity may require that those pages be moved to a private Internet provider.

### **Privacy Considerations**

The computer system and network are shared by all members of the University community. Because it is a shared resource, individuals should use the system responsibly in pursuit of University-related functions and in doing so, should not infringe on the rights, integrity, or privacy of others or their data. The ability to use the network and the system in no way exempts anyone from the necessities of ethical behavior and responsible use in the University community.

The University does not guarantee the privacy of users, their electronic files, or their communications. The University reserves the right, as owner, to preserve, monitor or inspect for business purposes any information transmitted through or stored on any technologically platform, and may do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses, malware, and other intrusive software), or to audit the use of University resources. In cases of misuse, the University also reserves the right to deny access to computing facilities.

When sources outside the University request an inspection and/or examination of any University-owned or -operated communications system, computing resource, and/or files or information contained therein, the University will treat information as confidential except:

- When approved by the appropriate University official(s) or the department head to whom the request is directed; or
- When authorized by the owner(s) of the information; or
- When required by federal, state, or local law; or
- When required by a valid subpoena or court order.

When notice is required by law, court order, or subpoena, users will receive prior notice of such disclosures.

### **Electronic Communications**

Users are responsible for all communications they transmit through the University's computers, networks and systems. Users should exercise caution when downloading executable programs via electronic communications to prevent injecting computer viruses and other intrusive software into University computers and/or networks. The following are examples of prohibited activities:

- Forgery or attempting forgery of electronic communications;
- Attempts to read, delete, copy, or modify the electronic communications of other users;
- Sending or attempting to send harassing, obscene, or threatening electronic communications;

- Sending or attempting to send unsolicited junk mail, “for-profit” messages or chain letters;
- Knowingly replicating or transmitting computer viruses or otherwise deliberately damaging the systems or files of others;
- Flooding or attempting to flood a user’s mailbox;
- Violating copyright laws through illegal file sharing, use of torrents or any other software including proxies that would allow the bypassing of University security apparatus and sharing illegally obtained copyrighted material.

E-mail is an official medium for communicating with faculty, staff and students. All faculty, staff and students are responsible for checking their University issued e-mail accounts in a timely fashion and on a regular basis.

Users of University computing resources further agree not to engage in cyber bullying. Cyber bullying is an act of aggression that intentionally intimidates, harasses, or imposes a reasonable fear of harm to an individual or the individual’s property. Cyber bullying may also impose a clear disruption on the daily activities of an individual through malicious, hateful, threatening or harassing digital information and/or electronic communications, including, but not limited to, Learning Management System, text, instant, and e-mail messaging, cellular telephone communications, social media forum, and Internet chatrooms, blogs and other postings.

### **Allocation and Use of Technology Resources**

The Chief Information Officer, with recommendation and guidance from the Technology Advisory Council, is responsible for the general allocation and use of technology resources in accord with the University’s purpose and goals. Allocations of technology resources are made through the budget and planning process. In addition, the Technology Advisory Committee assists the Chief Information Officer by recommending general guidelines and institutional priorities for the allocation and use of technology.

The Chief Information Officer, or other individual designated by the President, has the authority and responsibility for the development of technology standards and guidelines to ensure effective implementation of this policy, and for evaluating the effectiveness thereof. The Chief Information Officer is also responsible for evaluating that the allocation and use of technology resources adequately addresses the needs of academic and administrative units.

*Approved 9/86*

*Last Revised 11/18*