



IT USE GUIDELINE

Computer and Network Use – General Guidelines

General guidance on the secure, responsible, and reasonable use of UA computer and network resources.

Effective as of: **7/1/2013**

Sponsor and Approvers:

Scott Montgomery - Sponsor

John McGowan, Ashley Ewing, IT Governance - Approvers

Status of Guideline: **Published**

Audience:

This IT Guideline should be observed by:

Students Faculty Staff

Contractors/suppliers

Other (specify) [Click here to specify "other"](#).

Statement of need and purpose:

This information is provided to assist users in making good decisions about how to use UA computing and network resources. Note: This Guideline supplements the Policy described in the Terms of Use for Computer Accounts. That Policy takes precedence in all cases.

The University of Alabama undertakes to provide access to local, national, and international sources of electronically generated, stored, and transmitted information and to promote a free and open atmosphere in which thinking and thoughtful people can exchange information and ideas with other thinking and thoughtful people, both on and off campus. To protect users and the University from criminal and civil liability and the potential expenses and harm to reputation that may result from such liability; to protect and preserve the work product of authorized users; and to encourage informed and considerate use of UA resources, this strongly recommended Guideline and corresponding Policy documents have been codified and approved by The University of Alabama.

Guideline:

Use of a University Computer Account

UA computer and network access accounts are provided for your personal use of computer applications related to your position as a faculty member, staff member, or student of the University of Alabama. You must not allow anyone else to use the account or the resources to which the account gives you access. Your use of the account indicates your agreement to use it in accordance with all local, state, and federal laws and all University of Alabama policies; to use the account for University purposes only; and to cease using the account when you leave the University or when you are no longer authorized. All activity on the account is subject to inspection to ensure compliance with stated policies.

Shared Resource

The University of Alabama computer and network services are available to all faculty, staff and students. Because of high demand for these resources, respect for the rights and needs of others are central to these guidelines. To ensure access and service for all users, account holders must refrain from any action which interferes with the system, such as:

- Using computer or network services for commercial purposes or for profit
- Sending excessive e-mail locally or over the network such as chain letters, advertisements or solicitations
- Knowingly installing or running a program that will damage or place an undue burden on the system
- Knowingly acting in a manner that will disrupt normal operations of computers or the network

Privacy

Technology should not be used in a manner that infringes upon an individual's right to privacy. The following restrictions are to protect your privacy, as well as the privacy of others. Account holders are prohibited from:

- Using computer or network services in a way that violates copyrights, patent protections or license agreements
- Gaining unauthorized access to information that is private or protected, or attempting to do so
- Attempting to identify passwords or codes, interrupting security programs, or attempting to do so
- Monitoring or tampering with another person's e-mail
- Reading, copying, changing or deleting another person's work
- Using another person's userid/password, or allowing others to use yours
- Attempting to gain system and/or network privileges to which you are not entitled

Respectful Exchange of Ideas and Information

Computer systems and networks allow for a free exchange of ideas and information. This exchange serves to enhance learning, teaching, critical thinking and research. While the constitutional right of free speech applies to communication in all forms, we encourage civil and respectful discourse.

Personal Responsibility

Each individual who obtains a computer/e-mail account, or uses the computers and network resources made available by The University of Alabama, must understand that he/she is accountable for the guidelines set forth in this document and other applicable policies or guidelines. In addition, account holders assume responsibility for:

- Protection of his/her password
- Reporting any breach of system security
- Reporting unauthorized use of his/her account
- Changing his/her password on a regular basis
- Frequently making back-up copies of your work to ensure against loss
- Clearly labeling works and opinions as his/her own before they are widely distributed

Responsible users should avoid actions that may make themselves or their University criminally or civilly liable to others.

A user should avoid any acts or omissions that might subject him/her to criminal penalties or to civil liability to pay money to others. A user will want to be aware, as well, that some acts or omissions that may subject him/her to criminal penalties or civil liability may also subject the University to criminal penalties or civil liability. A user should also know that, under law, he/she may be required to reimburse the University for any amount of money it must pay to another because of injury caused by your conduct. This document presents, by way of example, kinds of conduct most likely to bring down criminal penalties or civil liability. A user should be aware, however, that if any other state or federal law makes the user or the University criminally or civilly liable for certain conduct, that law still applies even if not specifically described herein; and if state or federal law prescribes certain consequences for certain conduct, the user and the University may suffer those consequences even if they are not described herein.

Responsible users will contribute positively to a free and open atmosphere for electronic discussion. Cruelty, obscenity, crudity, and offensiveness, for the sake of offensiveness, have no place in the public discourse of a University community, but not all emotionally hurtful, offensive or inconsiderate conduct is or ought to be subject to official punishment. Nevertheless, as members of the University community, we are all responsible to one another and to the thinking and thoughtful community of which each of us ought to be a valuable part.

Responsible users will be considerate of other users of computer resources and facilities. Users may not use any University of Alabama workstation with the intent to intimidate, harass, or display hostility toward others. Users are also asked to be sensitive to the displaying of material that others might find offensive. Persons violating these guidelines in public facilities may be asked to leave the premises. University faculty, staff, and students also may be subject to disciplinary action.

Use of software

Computer software is a form of intellectual property controlled by licenses that spell out clearly how it may be used and distributed. All members of the University community must follow all license provisions regulating the use and distribution of computer software. Use or distribution of software in

violation of license provisions may subject the violator to criminal and civil penalties, as well as to civil liability to the licensor. Consider the following examples. You should not run your software on two or more computers simultaneously, unless the license agreement specifically allows it. You should not copy software available through the colleges or University departments, for use at home or in the dormitories, unless the license agreement specifically allows it. You should not copy software for distribution among members of a class or for a friend, even if the purpose in sharing it is purely educational, unless the license agreement specifically allows it.

Use of networks

Networks are also a form of property controlled by agreements between providers and users. Thus, violating a term of such an agreement may bring down upon the violator and the University consequences similar to those already examined with regard to software. Furthermore, public networks are regulated, or subject to regulation, by state and federal government. Violating a state or federal regulation may bring criminal or civil penalties down upon the violator. Finally, you should know that transmitting defamatory utterances concerning a person, organization, or institution may subject the perpetrator and the University to civil liability to pay money damages.

Use of any University property for private gain: The University provides computer resources to promote its teaching, research and service missions. As with other resources, faculty and staff members are bound by state ethics law. Alabama Code 36-25-5(a) provides as follows:

No public official or employee shall use an official position or office to obtain direct personal financial gains for himself, or his family or any business with which he or a member of his family is associated unless such use and gain are specifically authorized by law.

Use of institutional data

Information critical to the operation of the University, regardless of its format, is an asset of the University and Measures should be taken to protect this asset from unauthorized modification, destruction, or disclosure, whether accidental or intentional.

Responsible users should avoid actions that may inflict needless expense upon their University or others. Computing resources (including, but not limited to, e-mail, application and instructional software, mainframe resources, local area networks, and access to external networks), like all resources, require regular expenditures of money for their purchase and maintenance, even though some of these resources, like network storage space, may seem invisible and, hence cost-free. As with all University resources, the University bears the responsibility and has the authority to allocate or otherwise limit access to computer and network resources in order to ensure their most effective and economical use. For your part, you should not do anything that will impair the operation of computers, terminals, peripherals, or networks. You should not do anything that you know or should know is wasteful of computing resources, including, but not limited to, sending advertisements for commercial enterprises, sending mass mailings, or chain letters, obtaining unnecessary output, maintaining unnecessarily excessive file storage creating unnecessary multiple jobs or processes, or creating unnecessary network traffic.

Responsible users should avoid actions that may destroy, endanger, or divert another's research or writing. Among the most valuable and most sensitive of the University's computer resources are the personal work and storage spaces assigned to users. The University treats electronically stored information, including personal files, as confidential and permits examination or disclosure of their contents only when authorized by the owner of the information or when required by local, state, or federal law. Under Alabama Code 13A-8-102, it is a crime to attempt or achieve access to, communication of, examination of, or modification of, to destroy, or to disclose, use, or take data, computer programs or supporting documentation. In plainer words, under pain of state law, none of us may use, transmit, change, or delete another user's files or software without permission or introduce destructive software, such as programs known as computer viruses, Trojan horses, or worms, into any computer, computer system, or network. In predicting the consequences of such conduct, we should also consider FACULTY HANDBOOK, APPENDIX "C" (Academic Misconduct Disciplinary Policy), pp. 88-91.

Compliance:

Compliance to Guidelines is voluntary but recommended. Not adhering to guidelines can cause disruption to services, security exposures, and/or adverse impacts to other users. Enforcement of guidelines is addressed when deviations cause issues for others or result in known and significant security exposures and are handled through the organizational management structure.