

University of Arkansas at Little Rock (UALR) Information Technology (IT)

Appropriate/Acceptable Use Policy (AUP) For Faculty/Staff/Students March 3, 2003

Information technology (IT) has the ability to distribute and examine a vast array of material with unprecedented speed. One requirement however, remains constant: all information technology use must fully respect the rights of the University and IT community members. This AUP is designed to guide faculty, staff and students in the acceptable use of network and information systems provided by the University of Arkansas at Little Rock (UALR). More importantly, it is meant as an application of principles of respect using UALR computer resources, other computer users, and for the medium itself.

The UALR community is encouraged to make innovative and creative use of information technologies in support of education and research. Consistent with other University policies, this policy is intended to respect the rights and obligations of academic freedom as well as to protect the resources of the University.

The University campus network is an open network and therefore cannot protect individuals against the existence or receipt of material that may be offensive to them. Those who make use of electronic communications are warned that they may come across or be recipients of material they find offensive. Those who use email and/or make information about themselves available on the Internet should be forewarned that the University cannot protect them from invasions of privacy and other possible dangers that could result from the distribution of personal information. IT and network facilities of the University are finite and limited. These facilities should be used wisely and carefully with consideration for the needs of others. When used appropriately, these tools can enhance dialog and communications. When used inappropriately or unlawfully, these tools can infringe on the rights of others.

Current use of IT parallels familiar activities in other media and formats and existing University policies already provide guidance. Using electronic media in the place of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor will it alter the guiding policies. University policies, which already apply to freedom of expression, privacy and related matters, apply to electronic expression as well. This IT Appropriate Use Policy (AUP) addresses circumstances, which are new or at least unfamiliar in the IT arena and augments rather than replace other applicable University policies.

DEFINITIONS

UALR IT Systems include the computers, terminals, printers, networks, modem banks, and related equipment, as well as data files or documents residing on disk, tape, or other media, which are owned, managed or maintained by Computing Services and/or faculty/staff of UALR. For example, IT Systems include institutional and departmental systems, IT systems managed by UALR Computing Services, faculty research systems connected to the campus network, the campus telephone system, and the University's campus network (which is designed and managed by Computing Services). Privately owned equipment, such as laptops, PDAs, and home computers are considered an IT System if attached directly or remotely to the campus network and/or is used to access the UALR campus network.

A User is any person, whether authorized or not, who makes any use of any IT System from any location. For example, this definition includes persons who access IT facilities via an off campus electronic network, as well as those who use an UALR dial-in network (e.g., the campus network/Internet) to connect a personal machine to any other networked system or service. An IT User is a user with authorization to access a UALR IT System(s). IT Users include UALR students, faculty members, staff members, and alumni or alumnae with accounts on IT systems.

A System Administrator is an individual with the authority to determine who is permitted access to a UALR department system or server. For example, UALR Associate Director of Networks is the UALR campus network system administrator.

Network Security Officer (NSO) is an individual charged with maintaining the security of the UALR campus network and as such, has the authority to investigate security violations to ensure that security policy is complied with.

PURPOSE

The purpose of IT is to further the research, education, and administrative functions of UALR. To achieve this purpose, these policies intend:

- To ensure the integrity, reliability, and performance of UALR IT Systems and network.
- To ensure that the UALR community of IT Users utilize the campus IT facilities in a fair and equitable manner with respect for the rights of the community at large.
- To ensure that IT Systems and network are used for their intended purposes.
- To establish sanctions and processes for addressing violations.

SCOPE

The IT AUP applies to all UALR IT Systems owned, managed or administered by UALR faculty, staff and students and any use of those systems. Many particular IT Systems (UALR's News and World Wide Web sites, campus email services, etc.) have service-specific policies, which apply in addition to this AUP. Please refer to postings available with each system to identify all applicable policies.

The policies described herein are those that the University uses in the normal operation of IT facilities and network. This document does not waive any claim that UALR may have to ownership or control of any hardware, software, or data created on, stored on, or transmitted through UALR IT Systems and network.

USE OF IT SYSTEMS

Proper Authorization.

Use of UALR IT Systems is restricted to authorized UALR 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.

Appropriate/acceptable Use

UALR IT Systems and network may be used only for their intended authorized purposes. For example, privately owned computers may not host sites for non-UALR organizations across the IT managed UALR network without specific authorization.

Official Electronic Communications

Student e-mail accounts are created within 24 hours of class registration and faculty/staff e-mail accounts created when the initial hiring documents are complete. UALR E-mail is the official means of electronic communication with students, faculty and staff. Important university-related information will be sent to individual e-mail accounts. Students are responsible for regularly reading e-mail messages. Types of communication include but are not limited to financial aid information, inclement weather closings, e-bills and payment deadlines, registration information, and library notices. The UALR E-mail System can be accessed at <http://mail.ualr.edu>.

Commercial Use

Without specific UALR administration authorization, activities using IT Systems and network for non-UALR commercial purposes are prohibited. This is not meant to restrict normal communications and exchange of electronic data, consistent with the University's education and research roles, that may have an incidental financial or other benefit for an external organization. For example, it is not appropriate to discuss products or services with companies doing business with UALR or to contribute to Facfocus discussing issues relating to commercial products.

Vendor Contracts

All use of UALR IT Systems and network must be consistent with all contractual obligations of the University, including limitations defined in software and other licensing agreements.

PRIVILEGES FOR IT USERS

Free Inquiry & Expression

UALR IT Users are afforded free inquiry and expression consonant with the purposes of the University.

Reasonable Confidentiality

UALR IT Users can expect reasonable confidentiality for particular data. Systems Administrators will identify categories of data, which will be managed as confidential on a particular IT System and they will make all reasonable efforts to maintain the confidentiality of that data. However, limited risks do apply to confidentiality, for example to technical limitations, software bugs, and system failures. Systems Administrators will take reasonable steps to inform IT Users of the limits to confidentiality for their respective IT Systems. IT Users are expected to become familiar with those limit and risks of confidentiality and to manage their confidential data accordingly. Confidentiality of data must comply with the State of Arkansas Freedom of Information Act.

RESPONSIBILITIES FOR ALL USERS

Unauthorized Use

Users must not permit or assist any unauthorized person to access IT Systems. For example, any non-UALR organization or individual without appropriate authorization may not use UALR IT Systems. Each campus user must have and use a unique logon/password to a campus IT system. Multiple user logons or passwords are in violation of this policy.

Security

Users must not defeat or attempt to defeat any UALR IT System's security, for example, by "cracking" or guessing user identifications or passwords, compromising room locks or alarm systems, utilize software that will probe a network user system, or a sniffer gathering logon/password data.

Unauthorized Data Access

Users must not access or attempt to access data on any UALR IT System they are not authorized to access. Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept data communications not intended for that user's access, for example network sniffing or wiretapping.

Concealed Identity

Users must not conceal their identity when using UALR IT Systems. Users must use their own login ID and password.

Denial of Service

Users must not deny or interfere with or attempt to deny or interfere with service to other users, on campus or off campus, by means of "resource hogging," deliberate distribution of computer worms or viruses, or modification of any IT system. Knowing or reckless distribution of unwanted mail or other messages is prohibited.

Copyright

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

External Data Networks

Users must observe all applicable policies of external or off campus data networks when using such networks.

Modification of Data or Equipment

Without specific authorization, users of UALR IT Systems must not cause, permit, or attempt any destruction or modification of data or computing or communications equipment, including but not limited to alteration of data, reconfiguration of control switches or parameters, or changes in firmware. "Specific authorization" refers to permission by the owner or Systems Administrator of the equipment.

Personal Account Responsibility

Users are responsible for the security of their IT System accounts and passwords. Any user change of passwords must follow published guidelines. Accounts and passwords are assigned to single users and are not to be shared with any other person without authorization by the Systems Administrator. Changing another person's password is considered a form of harassment and unethical behavior.

Users are presumed to be responsible for any activity carried out under their IT System accounts.

Responsibility for Content

Representatives of IT publish "official" information in a variety of electronic forms. A statement of the Certifying Authority publishing the information will normally identify such official information. A Certifying Authority is that IT department or individual who certifies the accuracy of an electronic document and IT appropriateness for the conduct of IT business.

Users also publish information in electronic forms on IT equipment and/or over UALR's networks. UALR does not have any intention or opportunity to screen such private material and thus cannot assure IT accuracy or assume any responsibility for this material. Any electronic publication provided on or over UALR equipment and/or networks, which is not legitimately identified by a Certifying Authority, is the private speech of an individual user. Offensive content is to be reported to the Network Security Officer (NSO) for investigation.

Email use

The University's electronic mail facilities 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 or federal law.
- To perform an operation or activity that degrades the performance of the UALR's IT systems and/or network.

Threats and Harassment

Users may not use a UALR IT System to threaten or harass any person. A user must cease sending messages or interfering in any way with another user's use of IT Systems if the aggrieved user makes a reasonable request for such cessation.

Removal of Equipment or Documents

Without specific authorization by the System Administrator, users must not remove any University-owned or administered equipment or documents from an IT System.

Foreign Devices

Without specific authorization by the System Administrator, users must not physically or electrically attach any foreign device (such as an external disk, printer, network sniffer, sniffer software, network monitoring software, modem, or video system) to an IT System.

Violations

Users must not conceal or help to conceal or "cover up" violations by any party.

Users are expected to report any evidence of actual or suspected violation of this policy to the Systems Administrator of the facility most directly involved. In case of doubt, the report should be made to the UALR Network Security Officer (NSO) and/or UALR Chief Information Officer (CIO).

Reporting of Security Violations

If a user observes and/or suspects a security violation, he/she is obligated to report such to the UALR Network Security Officer.

IT RIGHTS

Personal Identification

Users of IT Systems must show identification including University affiliation upon request by a System Administrator, NSO, or University authority.

Access to Data

Users must allow systems administration personnel access to data files on IT Systems for the purpose of making backups, diagnosing systems problems and investigating policy and/or campus network security violations.

Oversight Authority

UALR NSO is authorized to investigate alleged or apparent violations of UALR IT policy or applicable law involving IT Systems and/or network using whatever means appropriate. The NSO will maintain a log and incident reporting of all such incidents. Any emergency action will be logged and security incident appropriateness reviewed after the fact.

Enforcement Procedures

The University may restrict the use of its IT and network systems when faced with evidence of violation of University policies, federal or local laws. The University reserves the right to limit access to its networks and IT systems. The University may limit access to material posted on University owned IT systems that is deemed inappropriate or not in keeping with the educational, research and community service missions of this University. Systems Administrators are authorized by the University Network Security Policy to apply certain penalties to enforce applicable policies. Such penalties include temporary or elimination of access privileges, which may apply to networks and other IT services or facilities.

When a Systems Administrator believes it necessary to preserve the integrity of facilities, user services, or data, he or she may suspend any account, whether or not the account owner (the user) is suspected of any violation. The System Administrator will attempt to notify the user of any such action.

If, in the opinion of the Systems Administrator, the violation warrants action beyond a System Administrator's authority, he or she may refer the case to other authorities, such as the NSO, the University disciplinary body appropriate to the violator's status, or to an employee's supervisor.

End of UALR Information Technology Services Appropriate Use Policy