TECHNICAL SERVICES APPROPRIATE/ACCEPTABLE USE POLICY

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 IT community members. This policy is designed to guide faculty, staff and students in the acceptable use of network and information systems provided by the University of Arkansas at Pine Bluff (UAPB). More importantly, it is meant as an application of principles of respect using UAPB computer resources, other computer users, and for the medium itself.

The UAPB 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 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 nature of the communication, nor will it alter the guiding policies. University policies, which already apply to freedom of expression, privacy and related matter, apply to electronic expression as well. This IT Appropriate Use Policy addresses circumstances, which are new or at least unfamiliar in the IT arena and augments rather than replace other applicable University policies.

Definitions

UAPB IT Systems include the computers, terminals, printers, networks, and related equipment, as well as data files or documents residing on disk, cloud solutions, tape, or other media, which are owned, managed or maintained by Technical Services and/or faculty/staff of UAPB. For example, IT Systems include institutional and departmental systems, IT systems managed UAPB Technical 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 Technical Services). Privately owned equipment, such as laptops, iPads, PDA's and home computers are considered IT System if attached directly or remotely to the campus network and/or is used to access UAPB campus network.

A User is any person, whether authorized or not, who makes any use of any UAPB 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 UAPB's VPN access to connect a personal machine to any other networked system or service. An IT User is a user with authorization to access a UAPB IT System(s). IT Users include UAPB students, faculty members, staff members, and alumni or alumnae with accounts on UAPB IT systems.

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

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

Purpose

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

1. To ensure the integrity, reliability and performance of UAPB IT systems and network.

2. To ensure that the UAPB community of IT users utilize the campus IT facilities in a far and equable manner with respect for the rights of the community at large.

3. To ensure that IT systems and network are used for their intended purposes.

4. To establish sanctions and processes for addressing violations.

Scope

The IT Policy applies to all UAPB IT Systems owned, managed or administered by UAPB faculty, staff and students and any use of those systems. Many particular IT systems (UAPBs News and World Wide Web sites, campus email services, etc.) have service-specific policies, which apply in addition to this policy.

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 UAPB may have to ownership or control of any hardware, software, or data created on, stored on, or transmitted through UAPB IT systems and network.

Use of Information Technology Systems

Proper Authorization

Use of UAPB IT systems is restricted to authorized UAPB 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 and access.

Appropriate/Acceptable Use

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

Commercial Use

Without specific UAPB administration authorization, activities using IT Systems and network for non-UAPB commercial purposes are prohibited. This is not meant to restrict normal communications and exchange of electronic data, consistence with the University' education, clinical, and research roles, that may have an incidental financial or other benefit for an external organization. For example, it is appropriate

to discuss products or services with companies doing business with UAPB or to contribute to fact focused discussion relating to commercial products.

Vendor Contracts

All use of UAPB 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 and Expression

UAPB IT Users are afforded free inquiry and expression consistent with the purposes of the University.

Reasonable Confidentiality

UAPB 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. However, limited risks do apply to confidentiality of that data, for example to technical limitations, software bugs, and system failures. System Administrators will take reasonable steps to inform IT Users of the limit to confidentiality for their respective IT Systems. IT Users are expected to become familiar with those limits 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. **UAPB IT USERS SHOULD HAVE NO EXPECTATION OF PRIVACY.**

Responsibilities for All Users

Unauthorized Use

Users must not permit or assist any unauthorized person to access IT Systems. For example, any non-UAPB organization or individual without appropriate authorization may not use UAPB 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 UAPB IT System's security, for example, by "cracking" or guessing user identifications or passwords, 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 an UAPB IT System they are not authorized to access. User must not 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 UAPB 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.

Modification of Data or Equipment
Without specific authorization, users of UAPB 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 UAPBs networks. UAPB 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 UAPB equipment and/or networks, which is not legitimately identified by a Certifying Authority, is the private speech of an individual.

Offensive content is to be reported to Technical Services for investigation.

Email Use
The University's electronic mail facilities should <u>not</u> be used:

1. To send unauthorized mass mailings of any type.
2. To send rude, obscene, harassing, or illegal material, or material that in any way conflicts with the regulations of the University.
3. To send any material that in any way conflicts with state or federal laws.
4. To perform an operation or activity that degrades the performance of the UAPBs IT system and/or network.

Threat and Harassment
Users may not use a UAPB 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 Technical Services.

Information Technology Rights

Personal Identification
Users of IT Systems must show identification, including University affiliation, upon request by a System Administrator, Technical Services or other 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
Technical Services is authorized to investigate alleged or apparent violations of UAPB IT policy or applicable law involving IT Systems and/or network using whatever means appropriate. Technical Services 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 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 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 University disciplinary body appropriate to the violator's status, or to an employee's supervisor.

SOCIAL MEDIA POLICY

This Policy is intended to provide the University of Arkansas at Pine Bluff students with guidelines for appropriate online activity. Although this Policy cannot address every instance of inappropriate social media use, it is intended to offer guidelines to UAPB IT community members, thereby helping to avoid potentially costly mistakes online. The nature of the Internet is such that what you "say" online will be captured forever and can be transmitted endlessly without your consent or knowledge. Students should remember that any information that is shared online instantly becomes permanent and public.

Scope

This Policy applies to all UAPB IT users' use of the Internet, including participation in and use of social media, regardless of whether such use occurs in the workplace, classroom, labs, library, resident hall, or off campus and regardless of whether such use involves the University of Arkansas at Pine Bluff's electronic equipment or other property.

"Social Media" Defined

Social Media are online platforms and tools used for interaction between groups of people to share content, profiles, opinions, insights, experiences, perspectives, and media itself. The rapid speed at which technology continuously evolves makes it difficult, if not impossible, to identify all types of social media. By way of example, social media includes: (1) social-networking sites (i.e. Facebook, LinkedIn); (2) blogs and micro-blogs (i.e. Twitter, Blogger); (3) content-sharing sites (i.e. Google+, SlideShare); and (4) images sharing sites (i.e. PhotoBucket, YouTube). This list is for illustrative purposes only, however, and all online activity is governed by this Policy.

Application of Other Policies

All of the University of Arkansas at Pine Bluff's students policies apply to conduct that occurs online in the same way that they apply to conduct that occurs in the workplace, classroom, labs, library, resident halls or off campus use.

Association with the University of Arkansas at Pine Bluff

Users who identify themselves online as being associated with the University of Arkansas at Pine Bluff must comply with the rules set forth in this section. Federal law requires that, when endorsing or promoting the university, the user must disclose his or her affiliation with (i.e., a student at), the University of Arkansas at Pine Bluff. Thus, although the University of Arkansas at Pine Bluff appreciates the loyalty and enthusiasm of its users, individuals must disclose their affiliation if they endorse the University of Arkansas at Pine Bluff online. If you disclose your

affiliation or relationship with the University of Arkansas at Pine Bluff, for example in your online profile, you must use an appropriate disclaimer to make clear that you are speaking only on behalf of yourself and not on behalf of or as an agent of the University of Arkansas at Pine Bluff. An example of an appropriate disclaimer follows:

The opinions and viewpoints expressed are those of the author and do not necessarily represent the position or opinion of the University of Arkansas at Pine Bluff.

To ensure continuity of the University of Arkansas at Pine Bluff's message, users may not represent themselves to be speaking on behalf of the University of Arkansas at Pine Bluff unless expressly authorized to do so.

Respect university time and property. University computers and resources are reserved for university-related education and research.

Prohibited Conduct

Students are prohibited from engaging in any of the following in their online activities and posts using UAPB IT Systems resources:

- Making any false or misleading statements;
- Promoting or endorsing violence;
- Promoting illegal activity, including the use of illegal drugs;
- Directing any negative comment towards or about any individual or group based on race, religion, gender, disability, sexual orientation, national origin, citizenship, or other characteristic protected by law;
- Disclosing any confidential or proprietary information belonging to the University of Arkansas at Pine Bluff.
- Posting, uploading, or sharing any recording or images (including audio, pictures, and videos), taken in the workplace or at any University of Arkansas at Pine Bluff-sponsored event without express advance authorization.
- Do not use the University of Arkansas at Pine Bluff's name to promote a product, cause, political party or candidate.

Nothing in this Policy is intended to or will be applied in a manner that limits students' rights to engage in academic freedom in accordance to Technical Services Appropriate Acceptable Use Policy.

Duty to Report
Users have an ongoing duty to report any violations of this policy by any other users. The University of Arkansas at Pine Bluff considers the duty to report to be a critical component of its efforts to ensure the safety of its users and to preserve the University of Arkansas at Pine Bluff's reputation and goodwill in the community. Therefore, any user who fails to report any conduct that reasonably appears to be in violation of this policy may be subject to discipline for such failure.

University of Arkansas at Pine Bluff prohibits taking negative action against any user for reporting a possible deviation from this policy or for cooperating in an investigation. Any user who retaliates against another user for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including expulsion.

Questions about This Policy
Social media changes rapidly and there will likely be events or issues that are not addressed in this policy. If, at any time, you are uncertain about the application of this policy or if a question relating to the appropriate use of social media arises that is not fully addressed by this policy, you should seek the guidance of the appropriate person *before* posting or otherwise engaging online. When in doubt, users always should ask for guidance first because, once the information is online, it can never be deleted.