UNIVERSITY OF CENTRAL ARKANSAS
BOARD POLICY

Policy Number: 412

Subject: Computer Use

Date Adopted: 05/99 Revised: 08/13, 10/22

1. Introduction

The university provides an opportunity for students and other members of the university community to enhance educational experiences and expand academic knowledge by making available access to computer facilities and resources, including the Internet, e-mail, and the World Wide Web. Thus, technology places a significant amount of power and information in the hands of its users that carries an equal amount of responsibility. Therefore, the following policy has been adopted to define responsible and ethical behavior relating to use of computing facilities and resources at the university. The policy is applicable to all university faculty, staff, and students. As users of these resources, all faculty, staff and students are responsible for reading and understanding the policy.

As a part of the physical and social learning infrastructure, the university acquires, develops, and maintains a computing infrastructure consisting of computers, networks, and a variety of related support systems. These computing resources are to be used for university-related purposes, including but not limited to, the following:

- Direct and indirect support of the university's teaching, research, and service missions;
- Support of the university’s administrative functions;
- Support of student and campus life activities; and
- Support of the free exchange of ideas among members of the university community, as well as between the university community and the local, national, and world communities.

All information technology resources are the property of the university. Except for personally-owned computers, the university owns, or has responsibility for, all of the computers and internal computer networks used on campus. Users of university computing resources and facilities do not own the systems or the accounts they use when accessing university computers or systems. All existing federal and state laws and university regulations and policies apply, including not only those regulations that are specific to computers and networks but also those that may apply generally to personal conduct and state-owned property. Rules prohibiting misuse, theft, or vandalism apply to all software, data, and physical equipment, including university-owned data as well as data stored by individuals on university computing systems.

2. Appropriate Use Guidelines

The rights of academic freedom and freedom of expression apply to the use of university computing resources. So too, however, do the responsibilities and limitations that are associated with those rights. The use of university computing resources, like the use of any other university-provided resource and like any other university-related activity, is subject to the normal requirements of legal and ethical behavior.

Employee and student access to and use of electronic tools such as e-mail and the Internet are intended for university business and educational purposes. Limited and reasonable use of these tools for occasional employee personal purposes is permitted as long as the use does not result in additional cost or loss of time or resources for intended business purposes.

3. Inappropriate Uses

Faculty, staff, and students must use good judgment in the use of all computing resources, including but not limited to Internet access and e-mail use. E-mail messages must be appropriate in type, tone and content. Employee and student use of e-mail and the Internet must be able to withstand public scrutiny without embarrassment to the university or the State of Arkansas. Computing and telecommunications may be used only for legal purposes and may not be used for any purpose that is illegal, unethical, dishonest, damaging to the reputation of the university or likely to subject the university to liability.

Inappropriate uses of computing resources at the university include, but are not limited to, the following:

- Any activity that would adversely affect the proper function of the network or the use of the network by others;
- Illegal copying, sharing or transmission of copyrighted software or other material licensed or otherwise protected by copyright;
- Any activity that would cause another user to lose control or usage of a computer or account;
- Commercial or profit-making activities unrelated to the university's mission;
- Creating, transmitting, executing, or storing malicious, threatening, harassing, obscene, or abusive messages, images, programs, or materials;
- Misrepresenting an identity or affiliation;
- Violating university security, damaging university systems, or using computing privileges to gain unauthorized access to any university computer system and/or any computer system on the Internet;
- Any activity that violates federal, state, or local laws, policies or regulations;
- Fundraising for any purpose unless sponsored by an official university organization with appropriate university approval;
- Permitting another person to use one’s account;
- Accessing or using another person's account for any reason;
- Removing or defacing hardware, software, manuals, etc. from open computing labs; and
- Abusing computer networks or computers at other sites connected to the networks.

The individual account owner is responsible for proper use of the account, including password protection.

4. Right to Privacy:

The right to privacy of e-mail and other electronic files against unwarranted or unreasonable entry or search is a basic tenet of university policies. Electronic files may be accessed or entered (including e-mail files) under one or more of the following conditions:

- The user requests or gives permission to the university to access an account; or
- Pursuant to a valid search warrant or court order.

In the situations set forth below, access must be granted by at least two of the following individuals—director of internal audit; chief of police; associate vice president of human resources and risk management; or general counsel:

- An emergency situation exists in which the physical safety and/or well-being of a person(s) may be affected or university property may be damaged or destroyed;
- Reasonable grounds exist to suspect that a violation of law or university policy is occurring; or
- If necessary to maintain the integrity of the computer system or to protect the rights or property of the university.

Electronic files of former employees may be accessed or entered (including e-mail files) for purposes of continuity of university operations with approval of the appropriate vice president.

5. Disclaimer:

The university does not manage the Internet and is not responsible for offensive material that may be encountered. It is the policy of the university to abide by and follow federal and state laws. Disclaimers regarding departmental and individual pages are addressed in the Web Site Usage Policy. Views and opinions expressed in e-mail are strictly those of the authors. The university is not responsible for the content of e-mail communications.

6. Disciplinary Action:

Engaging in any activity that violates the Computer Use Policy may result in the immediate suspension of an individual's computer access privileges, other disciplinary and/or legal action. The imposition of any sanction imposed under this policy is subject to review pursuant to applicable provisions of the Faculty, Staff and Student Handbooks.