

**POLICIES AND PROCEDURES
OUACHITA TECHNICAL COLLEGE**

SUBJECT AREA: Information Technology
POLICY/PROCEDURE: Computer Use Policy
DATE: 28 November 2006
REVISION(S):

NUMBER: 6.02

PURPOSE

The intent of this policy is to provide the underlying philosophy and establish guidelines for the regulation of information technology resources that Ouachita Technical College (OTC) provides to students, faculty, staff, and associates of the College.

The availability of information technology resources at OTC will continue to expand as need dictates. Access to these resources is a privilege, not a right. Each person using the College's information technology resources must act responsibly and maintain the integrity of these resources.

The College reserves the right to limit, restrict, or extend the use of and access to the institution's information technology resources. Those who do not abide by the policies listed below, whether through deliberate disregard, negligence, or naiveté, should expect suspension of their privileges and possible referral to the appropriate judicial process. Users must behave responsibly in light of access to vast services, sites, systems, and people.

EXAMPLES OF MISUSE

Examples of misuse include, but are not limited to, the activities in the following list.

- Using a computer account that you are not authorized to use. Obtaining a password for a computer account with or without the consent of the account owner unless the account is designated for group work.
- Using the Campus Network to gain unauthorized access to any computer systems.
- Computing facilities, services, and networks may not be used in connection with compensated outside work or for the benefit of organizations not sanctioned by OTC. State law restricts the use of state facilities for personal gain or benefit.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting computing resources.

- Using electronic mail to harass others.
- Masking the identity of an account or machine.
- No one shall use the Campus computing resources to transmit fraudulent, defamatory, obscene messages, or sexually explicit materials. Sexually explicit materials shall not be accessed or displayed on any OTC computer, terminal or printed from any campus printer.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- Tampering, reconfiguring, moving or changing computer settings without permission.

PRIORITY IN USE OF COMPUTING RESOURCES

In the campus library and general-access computer labs, or in any other environment in which users must share computing resources, priority shall be given to users engaged in activities directly related to the College's mission, e.g. completing course assignments or engaging in research. The library and computer labs may adopt regulations to implement this policy and to encourage cooperation among users of the same equipment.

COMPUTER AND NETWORK STORAGE AREAS

Network storage areas are provided for the use of faculty, staff, and students. The content and maintenance of a user's storage area is the user's responsibility. As such, the user must:

- Keep the number of files to a minimum.
- Routinely check for viruses.
- Not store files or programs on any computer or server that is not related to OTC business.
- Keep privileged, confidential, or sensitive information from being disclosed for any purpose other than official OTC business.

ENFORCEMENT AND SANCTIONS

System administrators are responsible for protecting the system and users from abuses of this policy. Pursuant to this duty, system administrators may (1) formally or informally discuss the matter with the offending party, (2) temporarily revoke or modify access privileges, or (3) refer the matter to the appropriate disciplinary authority.

Any violation of this policy may result in the revocation or suspension of access privileges. Imposition of such a sanction is within the discretion of the Department of Information Technology or the appropriate academic or administrative unit.

Any violation of this policy is misconduct for the purposes of the Student Rights/Responsibilities, the College Rules as outlined in the College Handbook, and College personnel policies and may be punished accordingly.

Any offense that violates local, state, or federal laws may result in the immediate loss of all College computing and network privileges and may be referred to the appropriate disciplinary authority and/or law enforcement agencies.

ARKANSAS LAW

It is a violation of Arkansas code to access, alter, or damage any computer system, network, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization. It is also unlawful to knowingly and without authorization, disclose a password to any computer system, network, or to gain unauthorized access to a computer or to interfere with the operation of a computer, network, or to alter, without authorization, any computer software. Arkansas Code, Chapter 41, subchapter's 1 and 2 specifically address the following:

- 5-41-104. Computer trespass
- 5-41-202. Unlawful act regarding a computer
- 5-41-203. Unlawful interference with access to computers – Unlawful use or access to computers
- 5-41-206. Computer password disclosure

Disclaimer

Since the Internet is a global electronic network, there is no state/county control of its users or content. The Internet and its available resources may contain material of a controversial nature. Through this policy, OTC attempts to protect users from offensive information. However, ultimately, users must assume responsibility for their use.

OTC cannot control the availability of information links that often change rapidly and unpredictably. Not all sources on the Internet provide accurate, complete, or current information. Users need to be good information consumers, questioning the validity of information.

Also, OTC assumes no responsibility for any damages, direct or indirect, arising from use of its servers or from its connection to other Internet services.

AUTHENTICATION (Signature):

COPP

President

28 November 2006
(Date)

6.02