

**POLICIES AND PROCEDURES  
OUACHITA TECHNICAL COLLEGE**

**SUBJECT AREA: Information Technology**

**POLICY/PROCEDURE: Employee Acceptable Use Policy**

**DATE: 28 November 2006**

**NUMBER: 6.02**

**REVISION(S): 09/29/09**

**OVERVIEW**

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 faculty, staff, and associates of the College. This Acceptable Use Policy is not meant to impose restrictions that are contrary to the College's established culture of openness, trust and integrity. OTC is committed to protecting students, faculty and staff from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, storage media, network accounts providing electronic mail, are the property of OTC and the State of Arkansas. These systems are to be used for official college business purposes in serving the interests of OTC, and its mission of higher education.

Effective security is a team effort involving participation and support of every person who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

**PURPOSE**

The purpose of this policy is to outline the acceptable use of computer equipment at OTC. These rules are in place to protect the individual and OTC. Inappropriate use exposes OTC to risks including virus attacks, compromise of network systems and services, and legal issues.

**SCOPE**

This policy applies to faculty, staff, and other employees of OTC. This policy applies to all equipment owned or leased by OTC and personal equipment attached to any network maintained by OTC.

**GENERAL USE AND OWNERSHIP**

While OTC's administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the College systems is subject to the policies of the college. Because of the need to protect OTC's network, administration cannot guarantee the confidentiality of information stored on any network device belonging to OTC.

For security and network maintenance purposes, authorized individuals within OTC may monitor equipment, systems and network traffic per COPP 6.01. OTC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### **UNACCEPTABLE USE**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of OTC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing OTC owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

### **PROHIBITED SYSTEM AND NETWORK ACTIVITIES**

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by OTC.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which OTC or the end user does not have an active license is strictly prohibited.
- 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 and equipment for personal gain or benefit.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
- Knowingly running, installing or introducing on any computer system or network, a program intended to damage or to place excessive load on a computer system or network is prohibited. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms.
- Revealing your account password to others or allowing use of your account by others is prohibited. This includes family and other household members when work is being done at home.
- Using an OTC computing asset to actively engage in procuring, transmitting or displaying material that is in violation of sexual harassment or hostile workplace laws is prohibited. This includes, but is not limited to, pornographic, obscene, fraudulent, and defamatory messages or images.

- Effecting security breaches or disruptions of network communication is prohibited. Security breaches include, but are not limited to, accessing data of which the employee is not the intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior coordination is made with Computer Services.
- Executing any form of network monitoring which will intercept data not intended for the employee’s host, unless this activity is part of the employee’s normal duties is prohibited.
- Circumventing user authentication or security of any host, network or account is prohibited.
- Tampering, reconfiguring, moving or changing computer settings without permission is prohibited.

### **NETWORK STORAGE AREAS**

Network storage areas are provided for the use of faculty and staff. 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 data 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.

### **WORLD WIDE WEB ACTIVITIES**

A limited amount of bandwidth is available to the college for internet connectivity. As such, priority must be given to work-related communication, educational and professional development.

Personal browsing of acceptable websites is permitted provided that it does not affect an employee’s productivity or pose a threat to OTC’s network. As web threats change, so will the list of acceptable websites. As a general rule, the following activities are prohibited:

- Visiting sites that contain or promote pornography or gambling.
- Visiting sites that may violate local, state or federal laws.
- Participation in any peer-to-peer network without prior approval from computer services.
- Access to websites known as proxies or translators for purposes of circumventing established web filters.
- Access to sites that stream video or audio unless it is work related.

- Downloading of screensavers, background images or other executable packages from the internet for installation on any workstation without permission.
- Discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by OTC's Non-Discrimination and Anti-Harassment policy.
- When expressing personal beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of OTC.

## **EMAIL ACTIVITIES**

The use of email by users is permitted and encouraged when it supports the overall business objectives of the College. The overall objectives of this section are to comply with all applicable laws and regulations, to encourage a safe and pleasant working environment for all users, to minimize email service disruptions and to prevent unnecessary strain being placed on OTC's computer and telecommunications resources.

### **APPROPRIATE USE OF EMAIL**

- Email users are expected to check email accounts and to respond to messages on a regular basis.
- Users should use the email system to send and receive relevant business information which is in line with the responsibilities of their position.
- Users are expected to manage their mailbox by organizing messages and deleting emails that are no longer required.

### **INAPPROPRIATE USE OF EMAIL**

- The use of email for illegal or unlawful purposes, including but not limited to, fraud, libel, harassment, the spreading of malware or obscene/defamatory content is prohibited.
- Users should not open unsolicited or unexpected file attachments.
- OTC's email system should not be used for personal business purposes or to broadcast personal opinions on political, religious or other non-business critical matters.
- Creating or forwarding "chain letters" or "pyramid" schemes of any type.
- Unauthorized use or forging of email header information.
- Posting the same or similar non-business related messages to large numbers of Usenet newsgroups or mailing lists.
- Users should not store large file attachments in their mailboxes. All large files should be stored on the local machine or their network drive.
- Users must not store any personal emails or personal files sent via email on their work computer or on the shared network.

## **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 Computer Services department or the appropriate academic or administrative unit.

Any violation of this policy is misconduct for the purposes of the 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.

### **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 material. 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
_____	29 September 2009
President	(Date)
	6.02