

**POLICIES AND PROCEDURES
OUACHITA TECHNICAL COLLEGE**

SUBJECT AREA: Information Technology
POLICY/PROCEDURE: System Monitoring
DATE: 28 November 2006
REVISION(S):

NUMBER: 6.01

SYSTEM MONITORING

College employees who operate and support information technology resources regularly monitor transmissions for the purpose of ensuring reliability and security of these resources and services and in that process might observe certain transactional information or the contents of electronic communications. Except as provided elsewhere in these policies or by law, they are not permitted to seek out transactional information or contents when not germane to system operations or support, or to disclose or otherwise use what they have observed.

In the process of such monitoring, any unavoidable examination of electronic communications shall be limited to the least invasive degree of inspection required to perform such duties. This exception does not exempt systems personnel from the prohibition against disclosure of personal or confidential information.

Users do not own accounts on campus computers but are granted the privilege of exclusive use of their accounts. Use of OTC computing resources for storage or transmission of data does not alter any ownership interest of the user or the College in that data. Users are entitled to privacy regarding their computer communications and stored data.

College officials will access electronic files, including E-mail files, only under one or more of the following conditions:

1. The user consents in writing to such access.
2. There is a valid search warrant or court order, or a request for electronic records that are open to public inspection under the Arkansas Freedom of Information Act.
3. There exists an emergency situation in which the physical safety and/or well-being of person(s) may be affected or College property may be damaged or destroyed. Responsibility for authorizing access rests with the Director of Information Technology or the Vice President Finance and Administration.
4. There exist reasonable grounds to believe that a violation of law or College policy is occurring or has occurred. Responsibility for authorizing access rests with the Director of Information Technology or the Vice President Finance and Administration.
5. Access is necessary for maintenance of computers, networks, data, and storage system; to maintain the integrity of the computer, network, or storage system; or to protect the rights of property or the College or other users. Authorized personnel may routinely monitor and log usage data, such as network session connection times and end-points, CPU and

disk utilization for each user, security audit trails, and network loading. In all cases, the privacy rights of users shall be protected to the greatest extent possible.

AUTHENTICATION (Signature):

COPP

President

28 November 2006
(Date)

6.01