

COMPUTER USE- For details, please see the **Employee Handbook** –www.midsouthcc.edu

Computer and networking resources are provided by Arkansas State University Mid-South to enhance teaching, learning, service, and the activities which support them. ASU MID-SOUTH is committed to a computing system which effectively meets the needs of users.

Individuals who are granted computing accounts or use the computer resources of the College accept responsibility with the access which is granted. Each user is expected to use accounts or resources for the educational or administrative purposes approved by the College. **Activities beyond these stated purposes are strictly prohibited.**

The Computer Use Administrative Directive for Arkansas State University Mid-South is stated below. Violations of this directive will be reviewed through established College judicial and administrative procedures and may result in a loss of access as well as other disciplinary or legal actions. Users may use the same procedures to challenge actions which restrict computer usage.

- Users shall access only those computer resources which have been authorized for their use and must identify computing work with their own names or other approved IDs so that responsibility for the work can be determined and users can be contacted in unusual situations.
- Access to the Internet is a privilege granted by ASU MID-SOUTH; it is not an automatic right which accompanies the payment of tuition and/or fees. Users shall act in a considerate and responsible manner.
- Users should minimize the impact of their work upon the work of others. One should not infringe on others' use of the facilities or deprive them of system resources. Recreational activities such as downloading music, video, and game files or joining in chat rooms are not allowed because they consume substantial network resources.
- Configurations of lab hardware and software shall not be altered. This would include but is not limited to the following:
 - Modifying backgrounds, wallpapers, icons, etc.;
 - Downloading and installing screen savers;
 - Installing Yahoo Messenger, ICQ, or other programs.
- Intentional introduction of a computer virus is a serious offense subject to the strictest disciplinary regulations of the College. Any user who is notified that a virus was detected on a diskette, must destroy the diskette or have an Information Systems staff member disinfect the diskette immediately.
- Inappropriate use of computer resources includes but is not limited to the following:
 - Sending or displaying obscene or offensive messages, pictures, language, graphics, songs, etc.;
 - Forwarding messages that have been identified as 'virus infected';
 - Harassing or insulting others;
 - Using someone else's account;
 - Eating or drinking in the computer labs.
- Users are responsible for the use of their computer and e-mail accounts. They should take advantage of available system protection measures such as passwords and be sure to log out to prevent unauthorized usage of their accounts.
- Users shall use computer resources only for authorized purposes. This directive shall not prevent informal communication among students, faculty, and staff. However, accounts shall not be used for private consulting or personal gain.
- Users shall not attempt to copy or destroy programs or files that belong to the College or other protected sources without prior authorization from the Vice President of Information Systems. Programs and data provided by the College may not be taken to other computer sites; individually owned programs and programs acquired at other computer sites cannot be used at the College without authorization.
- Users of software owned by the College must agree to abide by the limitations included in the copyright and license agreements entered into with vendors. Furthermore, it is the user's responsibility to become familiar with the specific copyrights and licensing agreements for each product before using it. If other arrangements are made with a vendor, users must abide by stated provisions.
- Those users who have access to privileged or sensitive information may not disclose that information for any purposes other than approved official College business.
- Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files will be private.

I have read the above Administrative Directive, understand its regulations, and agree to abide by them. I understand that violations of this policy may incur disciplinary procedures as outlined in the College Catalog and/or *Employee Handbook*.

Signature

Date