

**ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES**

---

I. General Principles

- A. The purpose of this policy is to outline the expectations of authorized users and to establish the parameters regarding the acceptable use of IT resources.
- B. Individuals who are granted user accounts or who use IT resources at the College accept the responsibilities that accompany such access. Each user is expected to use accounts and IT resources for educational, research, or administrative purposes; except as otherwise provided in this policy, activities unrelated to these purposes are prohibited. Use of IT resources in violation of the regulations set forth in this policy will be reviewed through established College procedures for student and employee misconduct. Restrictions imposed on usage of computer and network systems may be challenged through the same procedures.
- C. The College is committed to intellectual and academic freedom in connection with its IT resources. Computers and networks can provide access to resources on and off campus, including the ability to communicate with other users worldwide. Such open access is a privilege, much like access to books in the library, and requires that individual users act responsibly. Use of IT resources should always be legal and ethical, reflect academic honesty, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property, ownership of data, system security mechanisms, the right to personal privacy, and to the right of individuals to freedom from intimidation and harassment.
- D. All federal and state laws, as well as general College regulations and policies, are applicable to the use of computing resources. These include, but are not limited to, the Family Education Rights and Privacy Act of 1974, 20 U.S.C. § 1232g; the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510 et seq.; the Arkansas Freedom of Information Act, Ark. Code Ann. §§ 25-19-101 et seq.; and state and federal compute fraud statutes, 18 U.S.C. § 1030 and Ark. Code Ann. §§ 5-41-101 et seq. Illegal reproduction of software and other intellectual property protected by U.S. copyright laws and by licensing agreements may result in civil and criminal sanctions.

II. Administration of Computing Resources

A. In General

- 1. The College, in accordance with state and federal law and the policies of the Cossatot Community College of the University of Arkansas Board of Visitors and the University of Arkansas Board of Trustees, may control access to its information and the devices on which it is stored, manipulated, and transmitted.

2. The College has the responsibility to: (a) develop, implement, maintain, and enforce appropriate security procedures to ensure the integrity and privacy of individual and institutional information, however stored; (b) uphold all copyrights, patents, licensing agreements, and rules of organizations that supply information resources.
3. Responsibility for administering the College's IT resources and for the security of these resources rests with the Department of Information Systems Support (DISS) and units designated in writing by DISS.

#### B. Users

1. "Users" includes but is not limited to currently enrolled students; employees; authorized contractors, vendors, and guests; and other authorized users as determined by the College.

#### C. System Administrators

1. A systems administrator is any person designated, within any campus unit, to maintain, manage, and provide security for IT resources, including computers, networks, and servers.
2. System administrators shall perform their duties fairly, in cooperation with the user community and College administrators. They shall adhere to this policy and all other pertinent College rules and regulations, shall respect the privacy of users to the greatest extent possible, and shall refer disciplinary matters to appropriate College officials.

#### D. Data Collection

No information shall be routinely collected that is not required by system administrators in the direct performance of their duties, such as routine backup for system recovery.

#### E. Privacy of Electronic Files

1. Users do not own accounts on IT systems but are granted the privilege of exclusive use of their accounts. Use of IT resources for storage or transmission of data does not alter any ownership interest of the user in that data. Users are entitled to privacy regarding their computer communications and stored data.
2. College officials will access electronic files, including e-mail files, only under one or more of the following conditions:
  - a. The user consents in writing to such access.
  - b. 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.

- c. There exists an emergency 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 DISS, Vice Chancellor, or Chancellor.
- d. There exist reasonable grounds to believe that a violation of law or College policy is occurring or has occurred. Access will take place only after a reasonable effort has been made to obtain consent. Responsibility for authorizing access rests with the Director of DISS, Vice Chancellor, or Chancellor.
- e. Access is necessary for maintenance of computers, networks, data, and storage systems; to maintain the integrity of the computer, network, or storage system; or to protect the rights or property of the College or other users. Authorized personnel may routinely monitor and log usage data, such as network session connection times and endpoints, 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.

#### F. The Arkansas Freedom of Information Act

1. The electronic files, including e-mail files, of college employees are potentially subject to public inspection and copying under the state Freedom of Information Act (“FOIA”), Ark. Code Ann. §§ 25-19-101 et seq.
2. The FOIA defines “public records” to include “data compilations in any form, required by law to be kept or otherwise kept, ... which constitute a record of the performance or lack of performance of official functions which are or should be carried out by a public official or employee [or] governmental agency....” Ark. Code Ann. § 25-19-103(1). All records maintained in public offices or by public employees within the scope of their employment are presumed to be public records. Id. Various exceptions apply. See Ark. Code Ann. § 25-19-105.

#### G. Education Records

1. Records containing information directly related to a student are confidential and protected from public disclosure by the Family Educational Rights & Privacy Act, 20 U.S.C § 1232g, and the Arkansas Freedom of Information Act, Ark. Code Ann. § 25-19-105(b)(2).
2. No one shall access any such records maintained in an electronic format or disclose or distribute their contents in any manner inconsistent with federal and state law and College regulations.

### III. Use of IT Resources

## A. In General

This section does not cover every situation involving the proper or improper use of IT resources; however, it does set forth some of the responsibilities that a person accepts if he or she chooses to use those resources. The purpose of this section is to establish rules for the benefit of all users and encourage responsible use of computing resources.

## B. Use Without Authorization Prohibited

1. No one shall (a) connect with or otherwise use any IT resource without proper authorization; (b) assist in, encourage, or conceal any unauthorized use, or attempted unauthorized use, of any IT resource; or (c) misrepresent his or her identity or relationship to the College to obtain access to IT resources.
2. Users shall use only those IT resources that have been authorized for their use and must identify computing work with their own names or an approved means of identification so that responsibility for the work can be determined and users contacted, if necessary.

## C. Accounts

1. Users shall use their accounts for the purposes for which they are established, as well as personal communications. Accounts and other IT resources shall not be used for personal financial gain or benefit or for the benefit of organizations not related to the College, except: (a) in connection with scholarly pursuits, such as faculty publishing activities; or (b) in accordance with College policy on outside consulting for compensation.
2. Users shall not subvert restrictions associated with their accounts, such as quotas and levels of access.
3. No one shall give any password for any College computer or network to any unauthorized person, nor obtain any other person's password by any unauthorized means. Users are responsible for the use of their computer accounts and shall not allow others access to their accounts, through sharing passwords or otherwise. Users should take advantage of system-provided protection measures to prevent such access.
4. When a user is no longer a member of the campus community or is assigned a new position and/or different responsibilities within the College, his or her account and access authorization shall be reviewed. A user shall not use facilities, accounts, access codes, privileges, or information for which he or she is not authorized.

## D. Devices

1. The college provides access to devices to users for business and educational purposes consistent with the mission of the college. All users agree to comply

with all college policies and expectations of acceptable use of all college-owned devices.

2. All college-owned devices will be registered and managed by a centralized device management platform. IT Services will manage all device configuration and security policies using this platform.
3. Users will make no modifications to college-owned devices, including the configuration of hardware or software, without prior approval from DISS.
4. All users of mobile devices must employ reasonable physical security measures. Users are always expected to secure college-owned devices. This includes, but is not limited to, use of strong passwords, device encryption, and physical control of such devices whenever they contain college data.
5. In the event a device is lost or stolen, the user is required to report this event immediately to DISS and the campus police.
6. Users may be held financially responsible for the loss or physical damage to college-owned devices.

#### E. Security and Related Matters

1. No one shall (a) knowingly endanger or compromise the security of any College computer, network facility, or other computing resource or willfully interfere with others' authorized computer usage, (b) attempt to circumvent data protection schemes, uncover security loopholes, or decrypt secure data. (c) modify or reconfigure or attempt to modify or reconfigure any software or hardware of any IT resource, no matter where located, or to interfere with others' legitimate use of any such IT resource.
2. No one shall attempt to access, copy, or destroy programs or files that belong to other users or to the College without prior authorization, nor shall anyone use IT resources for unauthorized monitoring of electronic communications.
3. No one shall create, run, install, or knowingly distribute a computer virus, Trojan Horse, or other surreptitiously destructive program, e-mail, or data via any IT resource, regardless of whether demonstrable harm results.
4. Users shall not place confidential information in computers without protecting it appropriately. The College cannot guarantee the privacy of computer files, e-mail, or other information stored or transmitted by computer; moreover, the College may access such information in accordance with Part II of this policy. Users who have access to confidential or sensitive information shall disclose it only to the extent authorized by the Family Educational Rights & Privacy Act, the Arkansas Freedom of Information Act, and other applicable laws, and only in connection with official College business.

5. Users shall not knowingly or recklessly perform any act that will interfere with the normal operation of IT resources and shall not intentionally waste or overload IT resources.

#### F. Intellectual Property

No one shall copy, install, use, or distribute through IT resources any photographs, logos, images, graphics, graphic elements, audio, video, software, html markup, data files, or other information in violation of U.S. copyright, trademark, or patent laws or applicable licensing agreements. It is the user's responsibility to become familiar with the terms and requirements of any such laws or agreements. This subsection does not apply to any material that is in the public domain.

#### G. User Communications

1. Users assume full responsibility for messages that they transmit through IT resources.
2. No one shall use IT resources to transmit fraudulent, defamatory, or obscene messages, or any material prohibited by law.
3. No one shall use the College's IT resources to: (a) annoy, harass, threaten, intimidate, terrify, or offend another person by conveying offensive language or images or threats of bodily harm to the recipient or the recipient's immediate family; (b) repeatedly contact another person to annoy or harass, whether or not any actual message is communicated, and the recipient has expressed a desire for the contact to cease; (c) repeatedly contact another person regarding a matter for which one does not have a legal right to communicate (such as debt collection), once the recipient has provided reasonable notice that he or she desires such contact to cease; (d) disrupt or damage the academic, research, administrative, or related pursuits of another person; ~~or~~ (e) invade the privacy, academic or otherwise, of another person or threaten such an invasion; (f) Store, display, transmit, or intentionally solicit receipt of material that is or may reasonably be regarded as obscene, sexually explicit, or pornographic, except as such access relates to legitimate college-related academic or research pursuits or as needed to investigate violations of this policy or laws; (g) seek outside employment or participate in commercial activities or other forms of private financial gain; (h) campaign for public office or soliciting political contributions; (i) political lobbying, except for specific employees designated to lobby on behalf of a the UA System or one of its institutions; (j) participate in online gambling, wagering, or betting; (k) More than minimal use for private or personal purposes that interferes with work or job performance or that interferes with the activities of other employees, students, or other authorized users.
4. Users shall comply with this policy as well as the regulations and policies of any social media platforms and other public forums through which they disseminate messages.

5. Users shall not (a) initiate or propagate electronic chain letters; (b) engage in spamming or other indiscriminate mass mailings to newsgroups, mailing lists, or individuals; (c) forge communications to make them appear to originate from another person, e.g., spoofing; or (d) engage in resource-intensive activities unrelated to College functions, e.g., online role playing games (RPGs), listening to internet radio stations, connecting to any peer-to-peer file sharing network, etc.

#### H. Priority in Use of Computing Facilities

1. In general-access computer labs, or in any other environment in which users must share IT 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.

#### IV. Enforcement of Sanctions

- A. System administrators are responsible for protecting the system and users from abuses of this policy. Pursuant to this duty, system administrator 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.
- B. 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 DISS or the appropriate academic or administrative unit.
- C. Any violation of this policy is misconduct for purposes of the student code of conduct, the College personnel policies and may be punished accordingly.
- D. Any offense that violates local, state, or federal laws may result in the immediate loss of all privileges and may be referred to the appropriate disciplinary authority and/or law enforcement agencies.
- E. Any violation of this policy or UASP 285.1 shall be subject to the progressive discipline policy, College Policy 464 Uniform Conduct Standards. Depending on the severity of the violation, disciplinary action may include suspension or termination.

HLC Criterion: 2A; 2E

---

**Policy History:**

November 6, 2023	September 13, 2021
September 8, 2014	August 29, 2014
January 1, 2011	November 17, 2003

---

**PROCEDURE: NONE**