Acceptable Use of Technology Resources
Campus Procedure 810.0
Information Technology

I. Purpose and Scope

Access to computer systems and networks owned or operated by the University of Arkansas Community College at Batesville imposes certain responsibilities and obligations and is granted subject to University policies and local, state, and federal laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation and harassment.

II. Standard of Conduct

Users of UACCB's information technology resources are expected to abide by the following:

- Use technology resources only for authorized purposes. Access only information that is your own, that is publicly available, or to which you have been given authorized access.

- Protect your login credentials (e.g. username and password) and personal devices from unauthorized use. Never share your login password with anyone else. You are responsible for all activities on your username or that originate from your personal devices.

- Use only legal versions of copyrighted software, music files, videos, and other protected information in compliance with vendor license requirements and copyright law.

- Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, disk space, printer paper or other shared resources.

- Have up to date anti-virus installed on any personal computers that you connect to the campus network.

Users are NOT AUTHORIZED TO:

- Use or access another person's system, files, or data without explicit permission, use computer programs to decode passwords or access control information, or attempt to circumvent or subvert system or network security measures.

- Engage in any activity that might be purposefully harmful to information systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to University data.

- Use University systems for commercial or partisan political purposes, make or use illegal copies of copyrighted materials or software, store such copies on University systems, or transmit them over University networks.

- Use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by assuming someone else's identity.

- Waste computing or network resources, for example, by printing excessively or copying personal photos and videos files to network shares, etc.

- Use the University's systems or networks for personal gain; for example, by selling access to your credentials or to University systems or networks, or by performing work for profit with University resources in a manner not explicitly authorized by the University, or engage in any other activity that does not comply with the general principles described above.

- Physically attach personally owned devices to University equipment. Many of these devices can change the configuration of the equipment and cause potential issues. Some exceptions to this are authorized USB Flash drives (aka USB sticks or thumb drives), microphones, headphones, and USB phone chargers. If you have questions about the exception list, please contact our UACCB Help Desk.

III. Enforcements

The University considers any violation of acceptable use principles, policies or guidelines to be a serious offense. We reserve the right to copy and examine any files or information residing on University systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Violators are subject to disciplinary action as prescribed in the Student Code of Conduct Procedure 560.0, the Faculty Handbook and Code of Conduct and the Staff Code of Conduct. Offenders also may be prosecuted under laws including (but not limited to) the Communications Act of 1934 (amended), the Family Educational Rights and Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, the Electronic Communications Privacy Act, and the Arkansas Computer Related Crimes Act.

Any violation of UASP 285.1 or the University policy on use of technology resources shall be subject to the progressive discipline policy. Depending on the severity of the violation, disciplinary action may include suspension or termination.

IV. Information Ownership and Privacy

Individuals using computer systems owned by the University of Arkansas Community College at Batesville do so subject to applicable laws and University policies. Students and employees do not own their University computer accounts, but are granted use of them. The University will access an individual's electronic information if:

- the individual consents in writing to such access, OR

- there is an emergency which may affect someone's physical health or wellbeing, or may result in the damage or destruction of University property, OR

- there is reason to believe that a violation of law or University policy is occurring or has occurred, OR

- access is necessary for the maintenance of computers, networks, data, and storage systems, or to protect the rights or property of the University or other users.

Electronic information--including e-mail records--of University employees are potentially subject to public inspection and copying under the Arkansas Freedom of Information Act (FOIA) which states that, "All records maintained in public offices or by public employees within the scope of their employment are presumed to be public records."

V. Related Information

Campus Procedure 285.1 Cybersecurity; Campus Procedure 560.0 Student Code of Conduct, Faculty Handbook, Staff Handbook, Campus Progressive Discipline Policy.

Continuous improvement. The content of this document subject to regular review based on input from UACCB Information Services staff and the campus community. Suggestions for improvement should be directed to the Director of Information Services.

VI. Revision History

Effective Date: October 9, 2009
Revised Date: October 25, 2023
Review Date: October 25, 2024