Alderson Broaddus University
Acceptable Use Policy

Computing and Networking Resources Acceptable Use Policy

The Alderson Broaddus University Acceptable Use Policy (AUP) promotes the efficient, ethical, and lawful use of Alderson Broaddus University's computing and networking resources. The University's computing systems, networks and associated facilities are intended to support the University's mission and to enhance the learning environment. Alderson Broaddus University's policy regarding the appropriate use of University computing and networking facilities and the ethics of personal behavior apply to the use of all forms of electronic communication and access.

Rights and Responsibilities

Faculty, staff, and students may use University-owned computing equipment for instructional, research, or administrative purposes. Access to and use of Alderson Broaddus University computer facilities, campus telephone and data networks, electronically stored data, software, and the Internet shall comply with all federal and West Virginia state laws as well as the rules and regulations of the University. Misuse of these computer facilities, networks, software, and the Internet are violations of law and may be charged as such. By using Alderson Broaddus University's computing facilities, resources, networks, and the Internet, all users agree to the rules, regulations, and guidelines contained in this Acceptable Use Policy.

Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations. The University's computers and networks are a shared resource, for use by all faculty, staff and students. ***Any computer or network use that inhibits or interferes with the use of this shared resource by others is prohibited.*** The University will routinely review access logs, collect and analyze traffic data, and monitor network utilization to ensure reasonable use. Violations will result in immediate loss of computer and/or network privileges.

Students and employees may have rights of access to information about themselves contained in computer files stored in University-owned systems, as specified in federal and state laws. In addition, system administrators may access user files stored on University-owned systems as required to protect the integrity of the computer systems. Following organizational guidelines, system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged.

Students and employees shall be responsible for the backup and security of all user-created files. The Office of Information Technology (OIT) will regularly backup all files stored on designated file servers allowing for recovery of most lost or damaged files. However, the university will not be responsible for any user-created files that are unrecoverable.

It is a violation of this policy to:

- Intentionally and without authorization, access, alter, interfere with the operation of, damage or destroy all or part of any computer, computer system, computer network, computer software, computer program, or computer database.
- Give or publish a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network or database.
- Willfully exceed the limits of authorization and damage, modify, alter, destroy, copy, disclose, or take possession of a computer, computer system, computer network or any other University computing facility.
- Willfully, fraudulently and without authorization gain or attempt to gain access to any computer, computer system, computer network, or to any software, program, documentation, data or property contained in any computer, computer system or computer network.
- Use another person's name, password, identifying code or personal identification to access a computer system, network, or to send electronic mail.

University Provided Computer Resources

The following guidelines apply to anyone using computing resources provided by the University, including but not limited to computer labs, campus network, and Internet access:

- Loading of third-party software on any University-owned computer system is subject to authorization by the OIT.
- The transfer of copyrighted materials to or from any system, or via the University network without the express consent of the owner of the copyrighted material may be a violation of Federal Law, and is classified as a felony under State Law.
- University developed or commercially obtained network resources may not be re-transmitted outside of the University. Examples include newsgroups and Library databases such as ProQuest.
- It is the responsibility of each individual to protect his/her login and password for any computer-related account. The account holder is responsible for all activities to and from his/her account. The account holder may not share his/her account with anyone else and should never disclose his/her password to anyone for any reason.
- Any attempt to circumvent system security, uncover security loopholes, guess other passwords or access codes, or in any way gain unauthorized access to local or network resources is strictly forbidden and violation is grounds for immediate expulsion or termination from the University.
- Under no circumstances will any individual be permitted to use their network connection or computing privileges for commercial purposes. You may not advertise any commercial products. Any commercial use of University facilities is explicitly prohibited by the University and is grounds for the loss of network privileges.
- Inappropriate mass mailing is forbidden. This includes multiple mailings to mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing."

- Displaying obscene, lewd, or sexually harassing images or text (those without serious literary, artistic, political, or scientific value) in a public computer facility or location that can be in view of others is forbidden. Access to sexually explicit and other materials will be limited to no greater degree than access to print and visual materials found in most academic library collections.
- Interfering with, interrupting, or obstructing the ability of authorized users to use the University's computer or networking systems is prohibited.
- Networking equipment such as routers, switches, wireless access points, etc., or any computers serving as such devices may not be connected to the network without the explicit permission of OIT.

Private Computers Connected to the University Network (BYOD)

The following guidelines apply to anyone connecting their private computer to the University network.

- You, the owner of the computer, are responsible for compliance with all of the guidelines in the AUP as well as the behavior of all users on your computer, and all network traffic to and from your computer, whether or not you knowingly generate the traffic.
- A private computer connected to the network may not be used to provide access to the network for others who are not authorized to access the University systems. The private computer may not be used as a router or bridge between the University network and external networks, such as those of an Internet Service Provider.
- Should the networking staff of the University have any reason to believe that a private computer connected to the University network is using network resources inappropriately, network traffic to and from that computer will be monitored. If justified, the system will be disconnected from the network, and action taken by the appropriate authorities.
- Any residential student, with an authorized network account may use their residence hall connection for scholarly purposes, for official University business, and for personal use, so long as the usage: (1) does not violate any law or this policy, (2) does not involve extraordinarily high utilization of University resources, or substantially interfere with the performance of the University network, and (3) does not result in commercial gain or profit.
- Due to the possibility of a breach in the University's computer network security, students and employees are not permitted to connect a computer to the University's network and an external Internet Service Provider **AT THE SAME TIME**. Students who prefer to use an external ISP must notify OIT prior to connecting their computer to the external ISP network.
- Users are responsible for the security and integrity of their systems. In cases where a computer is compromised it is recommended that the system be either shut down and removed from the campus network as soon as possible in order to localize any potential damage and to stop the attack from spreading. **If you suspect electronic intrusion or hacking of your system and would like assistance contact OIT immediately.**
- The following types of servers should never be connected to the University network: DNS, DHCP, BOOTP, WINS, or any other server that manages network addresses. In addition, computers or devices providing web, FTP or other services designed to share files and/or

content may **not** be connected to the University network.

- The University will not be responsible for any damage to private computers, including hardware systems, software systems, files, and/or data that may result from connecting to the University Network
- In addition to all the guidelines contained in the AUP, users of the residence hall network must comply with the following regulations.
    - Use of a connection shall be limited to one computer at a time. Insuring proper use of the connection shall be the sole responsibility of the student to whom the connection has been assigned.
    - Software which allows "sniffing" of network packets is explicitly prohibited.
    - The user is responsible for defense against any and all viruses which may be propagated via the network, and it is recommended that an anti-virus program be loaded for protection. Problems with network connections should be reported immediately to OIT.

Cooperative Use

The Alderson Broaddus University computing environment is a shared resource. As such, all users of the University computer and network resources are urged to follow some basic guidelines to help enhance the work and learning of all who are a part of the University community.

- Users should refrain from overuse of information storage space, printing facilities, processing capacity, and/or bandwidth
- Users should refrain from overuse of interactive network utilities (video conferencing, gaming, etc.)
- Users should refrain from use of sounds and visuals, or any other activity, which might be disruptive to others
- Users should refrain from use of any computing resource in an irresponsible manner

Legal and Ethical Use

It is important that members of the University community be aware of the intellectual rights involved in the unauthorized use and copying of computer software. Alderson Broaddus University endorses the following statement of Software and Intellectual Rights that was developed through EDUCAUSE, a non-profit consortium of University's and universities committed to the use and management of information technology in higher education.

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution."

"Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade

secret and copyright violations, may be grounds for sanctions against members of the academic community."

Computer facilities and files owned by others should be used or accessed only with the owner's permission. Viewing or using another person's computer files, programs or data without authorized permission is unethical behavior and will not be tolerated. Such behavior, if used for personal gain, is plagiarism. Ethical standards apply even when the material appears to be legally unprotected. Improper use of copyrighted material may be illegal. The unauthorized copying of any software that is licensed or protected by copyright is theft.

Illegal uploading and downloading of copyrighted works through peer-to-peer (P2P) file sharing and other means of sharing and distribution are STRICTLY PROHIBITED.

A list of acceptable legal sites for downloading and using content is maintained by EDUCAUSE at http://www.educause.edu/legalcontent.

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.

Electronic Communications

The University provides e-mail (Gmail) and other communication tools through its learning management system (LMS), Moodle. Users should note that e-mail systems are not private secure communications. As such, e-mail users cannot expect privacy. By using the University LMS, each user acknowledges:

- The use of the LMS and electronic mail is a privilege not a right. The LMS is for University communication, research, or campus business. Transmitting certain types of communications is expressly forbidden. This includes chain letters, pyramids, and other messages of a similar nature; the use of vulgar, obscene or sexually explicit language and messages; sending harassing or threatening material; sending derogatory, defamatory or sexual or other harassment via electronic mail; or the use of the electronic mail for discriminatory communication of any kind; or the use of e-mail for commercial or political purposes; or the use of e-mail in conjunction with or as part of any criminal activity.

- Under the Electronic Communications Privacy Act, tampering with electronic mail, interfering with or intercepting the delivery of mail, and the use of electronic mail for criminal purposes may be felony offenses, requiring the disclosure of messages to law enforcement or other third parties without notification.

- E-mail messages and other electronic communications should be transmitted only to those individuals who have a need to receive them. Distribution lists should be constructed and used carefully. E-mail distribution lists should be kept current and updated regularly. Spamming is strictly forbidden.

- University e-mail accounts will be disabled for any of the following reasons and effective;
  - -On the day the student withdraws from the University
  - -On the day the employee ceases to be employed at the University
  - -Immediately on the day the University determines an e-mail account has been dormant for 6 months, constituting an abandoned account.
  - -Prior graduates of the University may maintain their e-mail account until such time as;
    - -The University determines the account holder is not adhering to University policies
    - -The e-mail account holder failed to enroll in required 2-step verification
    - -The account is considered abandoned.

Effective March 20, 2023: Students who graduate from the University will have 30 days from the date of Commencement before their e-mail account is disabled.

Waiver of Rights

All users who access Alderson Broaddus University computing resources waives any right to privacy and consents to access and disclosure by authorized University personnel of any electronic files, email, or any other transmissions created, stored, or transported using University computing resources. The University reserves the right to monitor and, if necessary, disclose the contents on a need-to-know basis of any electronic transmission, file, or communication for the purposes of troubleshooting, preventing system misuse, assuring compliance with policies, and complying with legal and regulatory requests for information. Users should recognize that under some circumstances, as a result of investigations, subpoenas or lawsuits, the University might be required by law to disclose the contents of electronic communications.

Disclaimer

The University may adopt further rules and regulations to implement this policy provided that no such rules or regulations shall be inconsistent with policy set forth above.

Reporting Violations of Computer Use Regulations

Violations of these regulations should be reported immediately to the Director of Information Technology Services, ext 6331. The University will make every effort to maintain confidentiality to the extent possible consistent with other obligations.

Disciplinary Action

Violations of these regulations will result in the appropriate disciplinary action, which may include loss of computing privileges, suspension, termination, or expulsion from the University, or legal action.