Acceptable Use Policy

Arkansas Christian Academy recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st Century technology and communication skills. To that end, we provide access to technologies for student and staff use.

This Acceptable Use Policy outlines the guidelines and behaviors that students are expected to follow when using technologies in school or when using their computer or other electronic device on the Arkansas Christian Academy campus. All technologies provided by or used at Arkansas Christian Academy are intended for educational purposes.

Students are expected to follow the Biblical mandate to honor the Lord Jesus Christ in all that they do. Therefore, students are expected to use technology in ways that are appropriate, safe, and cautious. Students are expected not to attempt to circumvent technological protocol measures. Further, students are expected to ask appropriate school personnel, should questions arise regarding matters pertaining to the use of these devices and their environments.

General Guidelines

The Arkansas Christian Academy wireless network is intended for educational purposes only.

- All activity over the network or using school technologies will be monitored and may be retained.
- Access to online content via the network is restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Arkansas Christian Academy issued devices are the only electronic devices allowed in the classroom. Personal devices such as laptops, iPads, phones, etc. are not permitted except during a student's concurrent period, in which case arrangements have been made with school administration.
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources may result in disciplinary action.
- Arkansas Christian Academy makes a reasonable effort to ensure student's safety and security online but will not be held accountable for any harm or damages that result from the use of school technologies.
- Users of the Arkansas Christian Academy network or other technologies are expected to alert school faculty or administration immediately of any concerns for safety or security.

Using Your Chromebook or other Electronic Device at School

School-issued Chromebooks may be used at school each day and should be brought in a fully charged condition. In addition to teacher expectations for the use of these devices, school messages, announcements, planners, calendars and schedules may be accessed using these devices.

Screensavers/Background photos
Users of electronic devices are expected to choose appropriate wallpapers, screensavers, desktop, backgrounds, and/or displays for their devices which are consistent with the school's core values and mission.

Downloading Apps, Music, & Sound

Teachers may require students to download apps or electronic books that have application to their specific course content.

On school-owned Chromebooks and devices, students may not download music from iTunes or any other music sharing site unless directed by or with the permission of a teacher. On all school-owned devices, sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.

Gaming
Students may not play games or use gaming apps during school instructional time without approval. School administration, faculty, and staff always reserve the right to ask students to close their devices and/or do random checks of school devices.

Saving Work
It is the student's responsibility to ensure that work is not lost due to equipment failure, failure to back-up files or deletion. Device malfunctions are not an acceptable excuse for not submitting work. Students should back up all work for their own protection.

Inspection
Students may be required to provide their technology for inspection at any time.

Internet Access
Students should not connect to the Internet using a detected hot spot or other unapproved wireless network while at school.

Arkansas Christian Academy provides students with access to the Internet and its content but makes no guarantee that the school wireless network will be up and running 100% of the time. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing will be monitored, and web activity records may be retained.

Users are expected to respect that the web filters used are safety precautions and are not to be circumvented. If a user believes a site or content should not be blocked, the user should alert a member of school faculty or administration.

Email
Arkansas Christian Academy provides students with an email account for school-related communication. Email may be monitored, archived, and restricted based on school policy.

Students provided with email accounts should use email with care. Users should not send personal information or attempt to open files or follow links from unknown origin. Users are expected to exercise appropriate, safe, mindful, and courteous communication and should only communicate with others as allowed by Arkansas Christian Academy policy or their teacher.

Social / Web 2.0 / Collaborative Content
Recognizing the benefits collaboration brings to education, Arkansas Christian Academy may provide users with access to web sites, content and/or tools that allow collaboration, sharing, and messaging among users.

Posts, chats, sharing, and messaging may be monitored. Users are cautioned not to share personally identifying information online. (see Social Media Policy in the ACA Policy Manual)

Plagiarism
Users should not use content without appropriate citation. This includes usage of words and from the Internet or elsewhere. A misrepresentation of appropriate credit to the content's creator is considered plagiarism. All research should be appropriately cited. (See ACA Policy Manual)

Artificial Intelligence
Artificial Intelligence (AI) and Large Language Models (LLM) are emerging technologies, being integrated into workplace and educational settings. Like any new technology, AI has the potential to support and enhance learning. However, it also presents several unknown challenges and may be used in ways that substitute rather than stimulate a student's own thinking and learning.

To support healthy learning and study habits, students should not use AI to complete or revise schoolwork, unless specifically directed by the teacher, and AI should ***never*** be a substitute for student's own thinking or effort. Any use of AI without teacher or admin permission will be considered plagiarism.

Personal Safety
Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard personal information of themselves and others. Users should never agree to meet with someone in-person whom they met online without parental permission.

If a user encounters any message, comment, image, or other online content that causes concern for one's personal safety, it should immediately be brought to the attention of a school staff member.

Cyber-bullying
Harassing, denigrating, impersonating, pranking, excluding, and cyber-stalking are all examples of cyber-bullying. Cyber-bullying will not be tolerated. Sending emails or posting comments, images, and/or other content with the intent of scaring, hurting, or intimidating someone else can be considered cyber-bullying.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, can be a crime. These behaviors may also result in severe disciplinary action and loss of privileges. Remember network activities are monitored and retained. (See ACA Policy Manual)

Security
Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or distrusted origin.

If a user believes a device being used might be infected with a virus, they should alert the school office. The office will notify the IT department. A device user should not attempt to remove the virus using any means or methods.

Parent/Guardian Responsibilities
It is strongly suggested that parents communicate with students about values and the standards they should follow regarding the use of the Internet and all media information sources such as television, cell phones, electronic devices, videos, movies, and music.

Examples of Acceptable Use
Students will:

- Never leave their device unattended and will know where it is at all times
- Use school technologies for school-related activities
- Follow the same guidelines for respectful, responsible behavior online that they are expected to follow offline
- Treat school resources carefully, and alert staff if there is any problem with their operation
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies
- Alert a teacher or other staff member if threatening, inappropriate, or harmful content (images, messages, posts) is seen online
- Use school technologies at appropriate times, in approved places, for educational pursuits
- Cite sources when using online sites and resources for research
- Recognize that use of school technologies is a privilege and treat it as such
- Be cautious to protect the safety of themselves and others
- Help to protect the security of school resources
- Recognize all network activities are monitored by school personnel

This is not intended to be an exhaustive list. Users should use their own good judgment when using technologies related to the school.

Examples of UN-acceptable Use:

- Spamming (sending mass or inappropriate emails)
- Gaining access to other students' accounts, files, and/or data
- Using the school's Internet/Email accounts for financial or commercial gain or for any illegal activity
- Participating in credit card fraud, electronic forgery, or other forms of illegal behavior
- Vandalizing school equipment (any malicious attempt to harm or destroy hardware, software or data. This includes the uploading or creation of computer viruses or computer programs that can infiltrate computer systems and/or damage software components.
- Transmitting or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients
- Bypassing the Arkansas Christian Academy web filter through a web proxy, 3G, 4G or Hotspot
- Using another student's device without permission of that student and a faculty member

- Illegally installing or transmitting copyrighted materials
- Violating existing school policy or public law in any way
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials
- Using chat rooms, sites selling term papers, book reports, and other forms of student work
- Gaming during inappropriate times and/or using inappropriate games which contradict the school's core values and mission
- Attempting to find inappropriate images or content
- Engaging in cyber-bullying, harassment, sending sexually explicit photos, arranging to meet someone on-line, or disrespectful conduct toward others
- Trying to find ways to circumvent the school's safety measures and filtering tools
- Agreeing to a physical face-to-face meeting of someone met online
- Using school technologies for illegal activities or to pursue information on such activities
- Attempting to hack or access sites, servers, or content that isn't intended for student use

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

Arkansas Christian Academy will not be responsible for damage, harm or theft to student-owned electronic devices. While Arkansas Christian Academy employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Arkansas Christian Academy will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this Acceptable Use Policy may have disciplinary repercussions, including but not limited to:

- Suspension of computer privileges/loss of device for a period of time (in such case, a physical textbook may be assigned for student completion of work)
- Notification to parents
- Detention, suspension, or expulsion from school and school-related activities
- Legal action and/or prosecution