Technology Acceptable Use Policy (AUP)

Student Edition

Statement of Purpose

In partnership with parents,ACA believes that all students should have access to technology tools, resources, communication systems and services that support learning and preparation for our modern world. ACA and parents of ACA students partner together to ensure that students act in a responsible, efficient, courteous, and legal manner. Internet access and other online services, available to students and teachers, offer a multitude of global resources. Our goal in providing these services is to enhance the educational development of our students. We educate students about appropriate online behavior including awareness and response to cyber-bullying and interacting with others on social media/networking sites. In addition, we take steps to monitor and block access to inappropriate content, monitor safety and security when students use electronic communications, prevent unauthorized access including “hacking,” and prevent unauthorized disclosure, use and dissemination of students’ personal information. All school Internet use including student school accounts are filtered and monitored.

This Student Acceptable Use Policy (“Policy”) sets forth the guidelines governing the use of all ACA technology resources by students while on or near school property, in school vehicles and at school-sponsored activities on- or off-campus, as well as the use of all ACA technology resources via off-campus remote access.

ACA will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

ACA will hold ALL students responsible for their use of technology, whether school-provided or personal, and they are expected to act in an appropriate manner in accordance with campus procedures, ACA policy and procedures, and legal requirements. This applies to the use of all ACA technology resources by students while on or near school property, in school vehicles and at school-sponsored activities on-or off-campus, as well as the use of all ACA’s technology resources via off-campus remote access.

This Policy shall be used in conjunction with the Student Code of Conduct.

ACA reserves the right to modify the terms and conditions of this Policy at any time.

Using the Internet and Communications Systems

ACA provides technology resources to students for the express purposes of conducting research, completing assignments, and communicating to the faculty, staff, and others to complement their educational experience. Just as students must demonstrate proper behavior in a classroom or school hallway, they must also behave appropriately when using any ACA computer networks, personal electronic devices, personal device data plans, software or websites sanctioned or used by ACA, and any personal technology used in an educational setting. Access to ACA’s technology is a privilege, not a right. Students must comply with all standards set forth in this Policy at all times in order to maintain the privilege of using its technology resources.

Students and their parents are advised that any information stored on and/or sent through ACA's technology resources is the property of ACA. Accordingly, in connection with ensuring student safety, ACA network administrators and/or other appropriate personnel will engage in periodic reviews and searches of stored files and communications stored on ACA technology resources to maintain system integrity and ensure that students are complying with this Policy and using technology in a responsible and appropriate manner. Such reviews will include students' use of school-approved educational websites or software to ensure that they are using it in an appropriate manner consistent with ACA's expectations for such use. Students do not have a reasonable expectation of privacy over any information stored on ACA technology or on school issued accounts.

ACA may allow students to bring personal technology devices (i.e., tablets, e-readers, smartphones, smart watches, etc) for use during the school day for authorized curricular purposes. Students that use personal technology devices will be required to comply with all aspects of the Acceptable Use Policy and/or the Student Code of Conduct in the use of such devices at school. A student's personal technology device may be subject to search by campus administrators in connection with determining if a student has committed a violation of this Policy and/or the Student Code of Conduct.

ACA remains committed to integrating technology to enhance its curriculum for students, which it believes increases students' educational experience for them and allows for better preparation for job skills and college success. Access to the Internet enables students to use extensive online libraries, databases and websites selected by ACA for use in instruction.

Although ACA strives to ensure that any Internet access avoids any inappropriate material, students and their families should be aware that some material accessible on the Internet may contain information that is inaccurate, profane, sexually oriented, defamatory and potentially offensive to some. ACA does not condone any student accessing, or attempting to access, such material, and it remains deeply committed to safe Internet use. ACA takes steps to minimize students' opportunities to access such content, including the implementation of technology prevention measures, such as extensive content-filtering software, to restrict access to inappropriate content such as those that are illegal, obscene, or harmful to minors. Each ACA device with Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act ("CIPA") and/or as determined by the school administration. This software is not fail-safe, however, and while at school, ACA strives to ensure that students' Internet use is supervised, it is possible that the software may miss some content, or students may find a way around the software to access inappropriate material. For this reason, this Policy is strictly enforced, and students who misuse any ACA technology outside its intended purpose, including the use of school-recommended websites for purposes outside the educational intent, will be in violation of this Policy, which may lead to disciplinary consequences for the student.

With this in mind, ACA still believes that the benefits of allowing student access to the Internet to enhance the educational experience outweighs any potential harm to students.

<u>Proper and Acceptable Use of All Technology Resources</u>

ACA requires students to use all technology resources, including any websites or software used in the classroom, in a manner consistent with the following rules. ACA will hold students responsible for any intentional misuse of its technology resources, or any other failure to comply with the rules in this Policy. When using ACA technology systems outside the school, parents should strive to ensure that students do so in compliance with the rules set forth in this Policy, as ACA is unable to supervise students' technology use at home. Generally speaking, ACA's content-filtering software is limited to student's use of school technology on the school network, so parents are encouraged to place content-filtering software on their home computers or take any other steps necessary to monitor students' Internet usage at home.

Students, who unintentionally access inappropriate material in connection with their use of any ACA issued account or technology, including websites and software used in the classroom, shall immediately stop accessing the material and report it to a supervising adult. ACA shall take immediate steps to ensure such material is blocked from further view at school by its content-filtering software.

All ACA technology resources, including but not limited to school computers, communications systems and the Internet, including any websites or software used in the classroom, must be used in support of education and academic research and in accordance with the rules set forth in this Policy.

Activities that are permitted and encouraged include the following:

- School work and assignments;
- Original creation and presentation of academic work;
- Research on topics being discussed in classes at school;
- Research for opportunities outside of school related to community service, employment or further education;
- Reporting inappropriate content or harassing conduct to an adult.

Activities that are barred and subject to potential disciplinary action and loss of privileges, whether on a school-provided or personal electronic device, include the following:

- Attempting unauthorized access, or "hacking," of ACA computers or networks, or any attempts to bypass Internet content-filtering software used by ACA.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student is not an intended recipient or logging into a server or account that the student is not expressly authorized to access. For purposes of the section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, forged routing information for malicious purpose, and any other form of network monitoring designed to intercept data not intended for the student's host.
- Engaging in abusive, harassing, insulting, ostracizing, intimidating, or any other online conduct which could be considered bullying and/or damaging to another's reputation while using any ACA technology resource, to include the use of any website or software used by the school.
- Engaging in any conduct potentially constituting "cyberbullying," which means bullying done through the use of any electronic communication device, including the use of a cellular or other type of telephone, a computer, a camera, electronic mail, instant messaging, text messaging, a social media application, an Internet website, or any other Internet-based communication tool. Examples of cyberbullying include, but are not limited to:
    - Creating a social networking site or web page that masquerades as another person's personal site and using it to embarrass the other person.
    - Making it appear that a person is posting malicious comments about a friend to isolate the person from his or her friends.
    - Posting a person's personally identifiable information on a site to put the person at greater risk of contact by predators or strangers.
    - Posting abusive comments on someone's social networking site.

  - Recording and distributing media with the intent to manipulate or embarrass others.
  - Sending abusive comments while playing interactive games.
  - Sending abusive text messages to cell phones, computers, or Internet-connected game consoles.
  - Sending, posting, or sharing negative, harmful, false, or mean content about someone else.
  - Sending, posting, or sharing statements encouraging another person to commit self-harm.
- Engaging in any conduct that damages or modifies, or is intended to damage or modify, any ACA equipment, network, stored computer file, or software, to include any conduct that results in a person's time to take any corrective action.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control logs.
- Intentional or neglectful transmission or direct placement of computer viruses or other unauthorized programs onto ACA equipment, networks, stored computer files, or software.
- Interfering with or denying service to any other use or than the student's host (for example, denial of service attack).
- Participating in online chat rooms or using instant and/or text messaging without prior approval by a classroom teacher, coach or administrator.
- Port scanning or security scanning.
- Presenting any copyrighted, registered, or trademarked work as that of the student.
- Refusing to submit to a search of a personal electronic device in accordance with the Student Acceptable Use Policy and the Student Code of Conduct.
- Revealing an account password to others or allowing use of an account(s) by others. This includes family and other household members when work is being done at home.
- Searching, viewing, communicating, publishing, downloading, storing, or retrieving any inappropriate or offensive material, including but not limited to obscene, profane, vulgar, or pornographic materials, or any material that is not related to the permitted activities set forth above.
- Sharing online any personal information of another student or staff member, including name, home address, or phone number.
- Taking, disseminating, transferring, or sharing obscene, sexually oriented, lewd, or otherwise illegal images or other content, commonly referred to as "sexting."
- Tampering with, removing components from, or otherwise deliberately interfering with the operation of ACA computers, networks, printers, user files, or other associated peripherals.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which ACA or the end user does not have an active license.
- Using a website or software program implemented by ACA in a manner outside the scope of the use specified by the classroom teacher, coach or administrator.
- Using any programs/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet.
- Using any ACA technology for games, role-playing, multi-user environments, gambling, junk mail, chain mail, jokes or fundraising activities without prior approval by a classroom teacher or administrator.
- Using any ACA technology resource to engage in any activity that violates any Board policy, the Student Code of Conduct, campus rule, local, state, and/or federal law.
- Using any ACA technology resource to take, disseminate, transfer, or share obscene, sexually oriented, lewd, or otherwise illegal images or other content.
- Using any ACA technology resources for any commercial and/or for-profit purpose, to include personal financial gain or fraud.
- Using obscene or profane language on any ACA technology resource, to include posting such language on any website or software used by ACA.

- Using ACA or personal technology during the administration of state standardized testing, End of Course, and or final examinations unless expressly allowed to do so by a teacher.
- Using technology for plagiarism or otherwise representing the work of others as the student's own.
- Using USB, bootable CD's, or other devices to alter the function of any ACA technology equipment, network or software.
- Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations, including, but not limited to, any downloading, installation, or distribution of "pirated" or other software products.

Students shall immediately report any violations of this Policy to a classroom teacher or administrator. If any student or parent has any question about whether any activity may be a violation of this Policy, they should ask a classroom teacher or the Principal or designee.

Personal Electronic Devices

Personal wireless and mobile devices, in general, are not allowed. However, if a campus makes an exception for an academic or other reason specific to a student's need, the device may be provided filtered access to the Internet as well as access to any web-based student applications (e.g., Discovery Education Streaming, Moodle) that would normally be accessible to students from home. ACA is not responsible for the loss or theft of any personal electronic devices, or for damage, or unauthorized access to the device nor the data that resides therein. Students and parents assume any and all risks associated with bringing a personal electronic device to a campus or school-related event. In addition:

- All students with personal electronic devices being used for instructional or other school business must use ACA's wireless network, which is filtered according to federal guidelines for Internet access in public schools.
- If a student uses a personal electronic device in an inappropriate manner, he or she will lose their privilege of bringing a personal device to school. Additional consequences may be imposed based on the Policy and the Student Code of Conduct, as well as any campus-based consequences for violating the usage rules for personal electronic devices.
- Personal electronic communications such as e-mail, instant messaging, chat, blogs, etc., are prohibited at school unless the teacher and/or administrator has approved the use of an application for educational purposes.
- Personal electronic devices are never to be plugged into the wired network (i.e., computers, wall jacks, other school equipment, etc.).
- School officials may power on and search a student's device if there is a reasonable cause to believe that the device has been used in the transmission or reception of communications prohibited by law, policy, or regulation and if a student and parent have signed a form authorizing the student to possess the device at school.
- Sound on personal wireless and mobile devices must be turned off when it is being used as part of a class.
- Student selection of appropriate, tasteful screensavers and wallpaper is expected.
- Teachers will establish standards for personal electronic devices used in their respective classrooms; however, it is ACA's policy that students are not allowed to access the Internet unless supervised by a teacher or staff member.
- The student must take full responsibility for configuring and maintaining their personal electronic devices. ACA will not provide technical support for these devices.
- When personal electronic devices are not in the student's possession, the student must secure them. ACA will not store, nor will it accept responsibility for storing, any student's personal electronic device on school grounds. Personal electronic devices must go home with students daily.

Privacy and Security

Students are expected to use ACA's technology resources responsibly and in a safe and secure manner, regardless of whether such technology is accessed using a school-issued or personal electronic device. Students shall not share their individual logins, passwords, or access to ACA's technology with others without the prior approval of a classroom teacher or administrator. Students shall sign off or log off all ACA equipment, software, or Internet sites once they are done with their session in order to protect the integrity of their logins, passwords, or access.

Consequences

Violation of ACA's policies and procedures concerning use of the computer on the network will result in the same disciplinary actions that would result from similar violations in other areas of school policy, including the Student Code of Conduct. Any or all of the following consequences may be enforced if a student violates the terms of this policy:

1. Any disciplinary consequence, including suspension or expulsion, allowed under the Student Code of Conduct and deemed appropriate by ACA.
2. Denial, revocation, or suspension of a user's access to ACA's technology resources, with or without cause or notice for lack of use, violation of policy or regulations regarding acceptable network use, or as a result of disciplinary action against the user.
3. Referral to law enforcement authorities.
4. Termination of a system user account.

Violations of law may also result in criminal prosecution as well as disciplinary action by ACA. ACA will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the school's computer systems and networks.

Limitations of Liability

ACA makes no warranties of any kind, whether express or implied, for the technology resources it provides to students through ACA provided and/or a student's personal electronic device. ACA is not responsible for any damages that a student may sustain, including those arising from non -delivery of information, erroneous delivery of information, service interruptions, unauthorized use by a student, loss of data, and any potential exposure to inappropriate material from the Internet. Use of any information obtained through the Internet is at the student's own risk, as ACA makes no representations, and denies responsibility for, the accuracy or quality of the information. In exchange for being allowed to use ACA's technology resources, students and their parents hereby release ACA, its directors, employees, and representatives from any and all claims for damages that arise from the intentional or neglectful misuse of ACA's technology resources by the student.

Technology Acceptable Use Agreement

Student Edition

Acknowledgement Form

I have read, understood, explained, and discussed the Technology Acceptable Use Policy Student Edition with my child. ACA has taken precautions to eliminate controversial material. However, I also recognize it is impossible for ACA to restrict access to all controversial materials and I will not hold ACA responsible for materials transmitted on the network. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.	
Student Name:	
Name of Parent/Guardian:	**Date:**
I have read the Acceptable Use Policy and discussed it with my parent(s)/guardian(s).	
Student's Full Name:	