ACCEPTABLE USE POLICY (AUP) FOR TECHNOLOGY RULES AND REGULATIONS

Technology

Alabaster City Schools Board of Education provides students with access to technology in order to enhance student learning. The term “technology” as used in this document, is intended to have a broad interpretation. The term “technology” as used herein, includes, but is not limited to computers, networks, the Internet, electronic mail, instant messaging, electronic devices, mobile devices, wearable devices, hardware, software, and accounts. Although cell phones, smartphones and wearable technology can be used for many of the same activities as other forms of technology, additional rules apply to the possession and use of these communication devices.

This AUP applies to all technology, regardless of ownership, used on school property, during school hours or during other school-related activities. It also applies to the use of Board owned technology regardless of location or time of day.

Parental Restriction on Independent Internet Access

Parents of students under the age of 17, may request that their child not be allowed to independently access the Internet by notifying the school principal in writing within fifteen (15) school days of the student’s first day of attendance **each** school year. This restriction applies to the student independently operating any Board-owned technology to access the Internet. It does not prohibit the student from viewing Internet Sites presented by school staff or by other students as part of a lesson, or from using Internet-hosted software used by the school. In these cases, school personnel will take appropriate steps to restrict the student from using technology to access the Internet beyond the scope of the lesson or assessment. However, school staff cannot directly supervise every student every minute of the day they are on the computer.

Personally-Owned Technology

The use of any personally-owned technology at school is a privilege, not a right. The Board reserves the right to place conditions on, restrict, or prohibit the use of personally owned technology on its property. Students may only use personal technology during school hours when given specific permission to do so by their teacher or a school administrator. Prior to bringing any personal technology to school, students must first determine which devices their school allows on campus. Permissions may vary from school to school. All devices, software or accounts used to set up their own network for Internet access, such as wireless access points or “hotspots”, virtual private networks (VPNs), are prohibited at all schools.

School officials may read, examine, or inspect the contents of any such device upon reasonable suspicion that the device contains evidence of an actual or suspected violation of the law, of Board policy, of the Code of Student Conduct, or of other school rules, provided that the nature and extent of such examination shall be reasonably related and limited to the suspected violation. The school/school system is not responsible for the loss, damage, or theft of any electronic device brought to school or to a school event.

Rules and Limitations

Students should strive to be good “digital citizens”. In addition to following this AUP, school rules, and Board Policies, students must also comply with all applicable local, state, and federal laws when using technology. Any student identified as a security risk, or as having a history of such, may have their access to technology restricted or denied and may be prohibited from bringing personally-owned technology on campus.

Expectation of Privacy

Students should not expect that their files, communications, or Internet use while using Board-owned technology are private. Authorized staff may access, search, examine, inspect, collect, or retrieve information of any kind from the Board’s technology, at any time and without prior notice in order to determine if a user is in violation of any of the Board’s rules, or for any reason not prohibited by law. In addition, authorized staff may delete or remove a user’s files from Board-owned technology without warning when those files violate the AUP or when necessary to maintain safe and correct operations of the Board's Technology.

As noted above, school officials may read, examine, or inspect the contents of any personally-owned technology upon reasonable suspicion that the contents or recent utilization of the technology contains of an actual or suspected violation of the law, of Board policy, of the code of student conduct, or of other school rules, provided that the nature and extent of such examination shall be reasonably related and limited to the suspected violation.

Permission to Use Technology

In general, students while on campus should only use technology with a teacher or administrator’s permission for school related purposes.

Students must have specific permission in order to…

- Use personally-owned technology while in school.
- Publish information to websites, blogs, wikis, or other online workspaces. When doing so, students are expected to adhere to applicable design requirements, online safety practices, and general rules of good behavior.
- Take Board-owned technology off-campus. A permission form, including specific instruction and conditions, may need to be signed.

Examples of Unacceptable Use

This list does not cover every possible inappropriate action or use of technology. Students who engage in actions not specifically covered by this policy may be subject to appropriate disciplinary action in accordance with the Code of Student Conduct.

Students shall not:

1. Tamper with or modify technology, utilities, and configurations, or modify access control permissions, either with or without malicious intent.
2. Dispose of, move, or remove technology from its assigned location without the express direction or permission of the supervising teacher.
3. Disable, circumvent or avoid security measures, including the use of proxies to bypass Internet filters, log-on procedures, or any other security feature.
4. Send or intentionally receive files dangerous to the integrity of the network.
5. Intentionally damage, destroy, disable, or remove parts from technology devices. In such cases students or their families may be held financially responsible for the repair, replacement, or reconfiguration of affected equipment.
6. Intentionally damage, delete, destroy, or interrupt access to software or data files. In such cases, students or their families may be held financially responsible for the reinstallation, replacement, or reconfiguration of affected software and files.
7. Develop or install malicious software (on or off campus) designed to infiltrate computers, damage hardware or software,spy on others, or compromise security measures.
8. Disrupt the use of others by creating excessive network congestion through the use of online gaming, video, audio, or other media for non-school purposes.
9. Use technology in any way with the intention of annoying, bullying (i.e. cyberbullying), harassing, interfering with, or causing harm to individuals, institutions, organizations, or companies.
10. Install or download any software, including toolbars, without authorization.
11. Broadcast messages or participate in sending/perpetuating chain letters on networks.
12. Install or modify wireless connectivity devices such as wireless access points and routers.
13. Connect personal devices to system-owned or maintained equipment, or “tether”, in order to use Wi-Fi or cellular services, through which unfiltered Internet access may be gained.

Students shall not:

14. Attempt to obtain, steal, hack, or otherwise alter another user's login ID and/or password.
15. Access or use another user’s account, network credentials, resources, programs, files, or data.
16. Allow others to use your network account and/or password to access the network, email, or the Internet.
17. Use another person's identity or a fictitious identity.
18. Save information on any network drive or device other than your personal home directory or a teacher-specified and approved location.
19. Cause files to appear as if another person created them.
20. Forge or otherwise falsely reproduce or alter report cards, letters from the school, or other school system correspondence.
21. Forge or attempt to forge or “spoof” email messages.
22. Send or attempt to send anonymous email messages.
23. Use technology to cheat or plagiarize, or assisting others to cheat or plagiarize.
24. Send or request information including but not limited to hoaxes, chain letters, jokes, phishing scams, etc.
25. Intentionally waste supplies and materials.
26. Download games or play online games for personal entertainment rather than learning.
27. Use any System technology resource for personal gain, commercial, political, or financial gain.
28. Participate in personal, non-instructional, digital or online communications without the explicit permission and supervision of authorized school personnel (i.e. chat, email, social media, forums, text or instant messaging, blogging, etc.).
29. Create, access, view, or post to personal online accounts while at school.

<u>Students shall not:</u>

30. Intentionally use or steal another person’s technology device such as a cell phone, Chromebook computer, Chromebook equipment, (i.e., power adapter, power charger, cord, case, etc.).
31. Use inappropriate language, gestures, or symbols in any digital communications or files, including audio/video files.
32. Create, store, access, use, request, display, or post impolite, abusive, offensive, obscene, profane, racist, inflammatory, libelous, inaccurate, derogatory, malicious, insulting, embarrassing, bullying or threatening language, images, audio files, messages or other files.
33. Edit or modify digital pictures with the intent to embarrass, harass, or bully.

34. Link to external sites considered inappropriate by Board standards.
35. Intentionally view or encourage/enable others to view any material that may not have been filtered, but would be classified as inappropriate for the school environment whether on the Internet, or sent as an email attachment, or access from a digital storage device.
36. Commit the Board, any school, or any employee of the Board, to any unauthorized financial obligation. Any resulting financial burden will remain with the user originating such obligations.
37. Conduct communications about unlawful activities including references to illegal or controlled drugs, gun crimes, or violence.
38. Violate federal, state or local laws, including use of network resources to commit forgers, or to create a formed instrument (i.e. counterfeit money, fake identification, etc.).
39. Violate copyright laws, including illegally copying software, music, videos, and documents. (Students should become familiar with Copyright, the Digital Millennium Copyright Act, and Fair Use laws to ensure they fully understand the limitations of Fair Use rights).
40. Copy or use logos, icons, graphics, trademarks, or other legally protected data or images.

Students shall not

41. Use technology to compromise the personal privacy, reputation, identity, or safety of themselves or others.
42. Attempt to read, delete, copy, forward, or modify email or electronic files of others.
43. Post any false or damaging information about other people, the school system, or other organizations.
44. Falsely post as an employee of the Board of Education on any website, online forum,social networking site, or other online venue.
45. Post the image or intellectual property of others without their permission.
46. Post or expose the personal information of yourself or others. Personal information includes, but is not limited to a person’s full name, home or work address, phone numbers, and social security number.
47. Post your own full name or the full name of other students to a school website, blog, wiki, or other publicly accessible Internet site. When posting information about yourself or a fellow student, you may only use the first name and first letter of the last name of the individual. In addition, no information may be posted about a student if their parent or guardian has notified the school in writing that their child’s information cannot be posted on the web.

48. Make appointments to meet unknown individuals contacted via electronic communications.

Disciplinary Actions

Students are responsible for their behavior asit relates to technology. Therefore, students who are issued individual accounts shall take responsibility for keeping their login IDs and passwords secure.

School and/or System-level administrators will make the determination as to whether specific behavior has violated acceptable practices. Disciplinary actions for violating the AUP will be commensurate with those outlined in the Alabaster City Board of Education Student Code of Conduct and Attendance. In certain cases, financial penalties may apply.

Technology networks can provide individuals with access to location in the United States and around the world. Students should be aware that they may be liable for any violations of law committed while using technology.

The Alabaster City Board of Education will provide information about the use of its technology resources to local, State, or Federal law enforcement agencies or civil courts in accordance with applicable law.

Limitation on Liability

The Board makes no warranties of any kind; either expressed or implied, that the functions or the services provided by or through the Board's technology will be error free or without defect. The Board will not be responsible for any damage users may suffer, including but not limited to loss of data, failure to block or filter, or interruptions of service.

The Board will take reasonable steps to maintain the security of its technology; however, no assurance can be given that security breaches will not occur. Studentsshould report any suspected or actual breach of security.

Although the Board claims ownership of its various technology, all user-generated data, including email content and digital images, is implicitly understood to be representative of the author's individual point of view and not that of the school or school system. Students and their parents must also be aware that the Board cannot assume any liability arising out of the illegal or inappropriate use of technology.

Alabaster City Schools provides technology measures that include blocking or filtering internet access to visual depictions and text that are obscene, pornographic, or harmful to minors. These measures cannot be considered 100% effective. Students should report materials, images, etc. which they feel are inappropriate or a disruption of the learning environment to a teacher, school administrator, and/or to the Alabaster City Schools Information Technology Department.