STUDENT ACCEPTABLE USE POLICY (SAUP) FOR TECHNOLOGY: RULES AND REGULATIONS

Technology

Eufaula City Schools Board of Education (Board) 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, smart phones 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 SAUP 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 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/Computer hosted learning 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 rights 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 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, vandalism, 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 SAUP, 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 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 SAUP 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 the contents or recent utilization of the technology contains 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 should only use technology on-campus with a teacher or administrator's permission. During school hours, they should only use technology, whether the Board's or their own personal technology, 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 and appropriate digital citizenship.
- Take Board-owned technology off-campus. A permission form, including specific instructions and conditions, will be signed.
- Video, photograph, or record others.

Terms of the Required Use and Internet Safety Policy

Specifically, the student will adhere to these guidelines with district technology each time the Internet is used at home and on campus. 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:

1. Will make available for inspection by an administrator or teacher upon request any messages or files sent or received at any Internet location. Files stored and information accessed, downloaded or transferred on district-owned technology are not private.
2. Will not connect any personal technologies such as laptops and workstations, wireless access points and routers, printers, etc. to district owned and maintained local, wide or metro area network. Connection of personal devices and printers are permitted, but permission shall be granted by the ECS technology department prior to use and is not supported by ECS technical staff. Home Internet use and cost is the responsibility of the student both in cost and configuration.
3. Will keep devices secure and damage free. Each device is issued with a protective bag or case. Use of the provided protective bag/case is required at all times. This applies specifically to locations that have a one-to-one environment, where the devices will be assigned to and transported by specific individuals.
4. Will not send or intentionally receive files dangerous to the integrity of the network.
5. Will not 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. Will not 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. Will not 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. Will not 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. Will not 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. Will not install or download any software, including toolbars, without authorization.
11. Will not broadcast messages or participate in sending/perpetuating chain letters on networks.
12. Will not attempt to read, delete, copy, forward, or modify email or electronic files of others.
13. Will not post any false or damaging information about other people, the school system, or other organizations.
14. Will not falsely post as an employee of the Board of Education on any website, online forum, social networking site, or other online venue.
15. Will not post an image or intellectual property of others without their permission.
16. Will not 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.

17. Will not post your own full name or the full name of other students to a school website, blog, wiki, or other publicly accessible Internet site.
18. Will not make appointments or share location with unknown individuals contacted via electronic communications.
19. Will not attempt to obtain, steal, hack, or otherwise alter another user's login ID and/or password.
20. Will not access or use another user's account, resources, programs, files or data.
21. Will not allow others to use your network account and/or password to access the network, email, or the Internet.
22. Will not use another person's identity or a fictitious identity.
23. Will not save information on any network drive or device other than your personal home directory or a teacher-specified and approved location.
24. Will not cause files to appear as if another person created them.
25. Will not forge or otherwise falsely reproduce or alter report cards, letters from the school, or other school system correspondence.
26. Will not forge or attempt to forge or "spoof" email messages.
27. Will not send or attempt to send anonymous email messages.
28. Will not use technology to cheat or plagiarize or assist others to cheat or plagiarize.
29. Will not send or request information including but not limited to hoaxes, chain letters, jokes, phishing scams, etc.
30. Will not intentionally waste supplies and materials.
31. Will not download games or play online games for personal entertainment rather than learning at any time.
32. Will not use any system technology resource for personal gain, commercial, political, or financial gain.
33. Will not 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 instate messaging, blogging, etc.).
34. Will not create, access, view, or post to personal online accounts while at school.
35. Will not use inappropriate language, gestures, or symbols in any digital communications or files, including audio/video files.
36. Will not 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.
37. Will not edit or modify digital pictures with the intent to embarrass, harass, or bully.
38. Will not link to external sites considered inappropriate by Board standards.
39. Will not 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.
40. Will not 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.
41. Will not conduct communications about unlawful activities including references to illegal or controlled drugs, gun crimes, or violence.
42. Will not 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.).
43. Will not 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.)
44. Will not copy or use logos, icons, graphics, trademarks, or other legally protected data or images.

General Guidelines: Device Care

- Do not loan your device or charger and cords.
- Do not leave the device in vehicle.
- Do not leave your device unattended.
- Do not eat or drink while using the device or have food or drinks in close proximity to the device.
- Do not allow pets near your device.
- Do not place the device in the floor or in sitting areas such as couches or chairs.
- Do not leave the device near table or desk edges.
- Do not stack objects on top of your device.
- Do not leave the device outside or use near water such as a pool.
- Do not check the device as luggage at the airport.

ECS will at times perform maintenance on the devices by imaging. All files not backed up to server storage space or other storage media will be deleted during these processes. Students are ultimately responsible for backing up all personal files on their own storage media.

Disciplinary Actions

Students are responsible for their behavior as it 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 SAUP will be commensurate with those outlined in the Code of Student Conduct. In certain cases, financial penalties may apply.

Technology networks can provide individuals with access to locations in the United States and around the world. Students should be aware they may be liable for any violations of law committed while using technology. In accordance with applicable law, the Board will provide information about the use of its technology resources to local, state, and federal law enforcement agencies or civil court.

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. Students should 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 the Board cannot assume any liability arising out of the illegal or inappropriate use of technology.

Student Technology Provision

The student is responsible for the replacement of the charger, bag, case, and/or device in the event of theft. All damage incidents must be investigated by administration. Willful and deliberate damage to a device will result in a cost to the parent/guardian for the full amount of repair, or the complete replacement of the device. Damages may include the following:

- Damage as a result of violating the SAUP (i.e., involving food, drink, or other liquid on or near the device),
- Damage as a result of negligence (i.e., the device is placed in an unsafe location or position),
- Damage caused by misuse/improper handling (i.e., the device is dropped),
- Damage caused by a pet,
- Damage resulting in a broken screen. Subsequent broken screens will be charged at full cost,
- Damage caused by a service performed by anyone other than a representative of ECS or an Authorized Service Provider.

Parent/Student Acknowledgement Form

By signing the Parent/Student Acknowledgement Form for the **STUDENT ACCEPTABLE USE POLICY (SAUP) FOR TECHNOLOGY: RULES AND REGULATIONS**, the parent and student affirm that they have received and understands these rules and regulations and agree to abide by these SAUP rules and regulations and all other applicable Board policies.

Please Print	Please Sign
_____	_____
Student Name	Student Signature
_____	_____
Parent Name	Parent Signature

Date: _____