Bibb County Schools Technology Usage Policy for Students

Technology- Acceptable Use Policy (AUP)
Bibb County Schools (Board) provides students with access to technology in order to enhance student learning. The term "technology" refers to all forms of hardware, digital devices, software, and accounts. Although cell phones and smart phones 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 Restrictions 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 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.

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, including the use of personal online accounts. 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 or accounts used to set up their own network for Internet access, such as wireless access points, or "hotspots", are prohibited at all schools.
Keeping personal technology safe while in transit or at school is the responsibility of the owner. The school is not responsible for attempting to recover lost or stolen personal technology when students have not properly secured them in their school locker and/or personal vehicle.

Electronic Mail
The Bibb County School District provides access to electronic mail for all students over the age of 13 in grades 7-12. The network is used for class accounts on a limited basis. Access to e-mail is for class, and/or student use in any educational and instructional business that they may conduct. Electronic mail should reflect professional standards at all time. Bibb County Schools' e-mail accounts may not be used for political or personal gain. Bibb County Schools' e-mail accounts may not be used for attempting or successfully sending anonymous messages. Bibb County Schools' e-mail accounts may not be used for sending mass e-mails outside the system.

Rules and Limitations
Students should strive to be responsible "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.

Expectations 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.

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 evidence of a violation of these or other rules and policies, as well as any local, state, or federal laws.

Permission to Use Technology

In general, students should only use technology 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.
- Take Board-owned technology off-campus. A permission form, including specific instructions 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 may be held responsible for other inappropriate actions whether or not they are specifically included in this AUP.

Students shall not tamper, disable, damage, disrupt, or install…

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, logon 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, 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 System 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 WiFi or cellular services, through which unfiltered Internet access may be gained.

<u>Students shall not</u> invade, trespass, spy, falsify, cheat, waste, or use technology resources for personal purposes…

14. Attempt to obtain, hack, or otherwise alter another user's login ID and/or password.
15. Access or use another user's account, 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 a teacher-specified and approved location.
19. Cause files to appear as if they were created by another person.
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, 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> use Technology for improper, antisocial, unethical, or illegal activity…

30. Use inappropriate language, gestures, or symbols in any digital communications or files, including audio/video files.
31. 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.
32. Edit or modify digital pictures with the intent to embarrass, harass, or bully.
33. Link to external sites considered inappropriate by Board standards.
34. 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 accessed from a digital storage device.
35. 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.
36. Conduct communications about unlawful activities including references to illegal or controlled drugs, gun crimes, or violence.

37. Violate federal, state, or local laws, including use of network resources to commit forgery, or to create a forged instrument (i.e. Counterfeit money, fake identification, etc.)
38. 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.)
39. Copy or use logos, icons, graphics, trademarks, or other legally protected data or images.

<u>Students shall not</u> use Technology to compromise the personal privacy, reputation, identity, or safety of themselves or others…

40. Attempt to read, delete, copy, forward, or modify email or electronic files of others.
41. Post any false or damaging information about other people, the school system, or other organizations.
42. Falsely post as an employee of the Board of Education on any website, online forum, social networking site, or other online venue.
43. Materials that are offensive, threatening or that otherwise are intended to harass or demean recipients must not be transmitted, including jokes that are intended to offend, harass or intimidate.
44. Post the image or intellectual property of others without their permission.
45. 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 number, and social security number.
46. 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.
47. Make appointments to meet unknown individuals contacted via electronic communications.

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 AUP will be commensurate with those outlined in the *Bibb County Board of Education Student Code of Conduct and Related Policies*. In certain cases, financial penalties may apply.

Technology networks can provide individuals with access to locations in the United States and around the world. Persons should be aware that they may be liable for hurtful speech, invasion of privacy, copyright, and other violations in all 50 states and worldwide. The Bibb County Board of Education will cooperate with any properly executed request from any local, State, or Federal law enforcement agency 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 interruption 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 that the Board cannot assume any liability arising out of the illegal or inappropriate use of technology resources.

Acknowledgement Form

By signing the Student Code of Conduct Acknowledgement form, students and parents affirm that they have received and understand these rules and regulations. However, failure to sign or return a signed consent form does not release students from their obligation to abide by these AUP rules and regulations and all other applicable Board policies.

SOURCE: Bibb County Board of Education, Centreville, AL
ADOPTED: October 26, 1998
REVISED: July 29, 2009; June 20, 2013; July 12, 2016.