Limestone County Schools
Student Technology Acceptable Use Agreement

Technology
Limestone County Schools (District) 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 other personal technology devices can be used for many of the same activities as other forms of technology, additional rules ~~may~~ apply to the possession and use of these communication devices at school. This Acceptable Use Agreement (AUA) 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 District-owned or managed technology regardless of location or time of day.

Personally-Owned Technology
The use of any personally-owned technology at school is a privilege, not a right. The District 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.

When permitted by state law, cell phones, personal laptops, tablets, wearable technology, and other personal technology devices that could be used to distract, cheat, harass, or otherwise violate school rules must be in silent mode and kept out of sight in a locker, backpack, or other location away from students during school hours. Personal ear buds, headphones, and other personal listening devices may be used only for educational purposes with the express permission of a teacher or school administrator. Exceptions may be made by school or district administration to accommodate specific educational activities, in case of school or weather emergencies, or for medical necessity.

The following devices may not be brought to school under any circumstances:

- Any technology, such as wireless access points or personal hotspots, used to set up a network for Internet access
- Any technology which interferes with or adversely affects the functions or operations of the District's resources or infrastructure.

Students must follow all rules established by the transportation department regarding the use and storage of personal devices while on a school bus.

Students are responsible for keeping their device safe while in transit and at school. School staff and/or bus drivers will not be responsible for attempting to recover lost or stolen personal technology.

Expectations of Privacy
Students should not expect that their files, communications, or Internet use while using District-owned or managed technology are private. Authorized staff may access, search, examine, inspect, collect, or retrieve information of any kind from the District'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 District-owned or managed technology without warning when those files violate the AUA or when necessary to maintain safe and correct operations of the District'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.

Online Accounts & COPPA
Throughout the year, teachers may wish their students to use free, educationally-appropriate websites or apps that require individual accounts in order to enhance learning. In order to create the online account, the District may upload certain 'directory information' (see FERPA) to the provider; generally the student's name, school, and grade level. Due to the Children's Online Privacy Protection Act (COPPA) and other conditions, many websites require that minors first obtain their parent's permission before an account is established. The parent's signature on the Student Handbook Acknowledgement Form will be considered as granting this permission. Parents who do not wish to have student accounts established on websites pre-approved by the District must

submit a Restriction Letter to the school within five (5) days of the student's first day of attendance **each** school year (see Parental Right to Restrict).

Google Workspace for Education (GWFE) Services

As part of its technology program, Limestone County Schools will provide students in grades K-12 with a Google Workspace for Education (GWFE) account. GWFE accounts give students access to certain Google services in an environment managed by the school district. These services include an individual Google Drive, which provides students with online storage for files and web-based tools (a.k.a. Google Docs) for creating documents, collaborating, and researching. In addition, each student will receive a GWFE email account and calendar for school use. Limestone County Schools will issue all GWFE accounts and manage which features are made available to students. This includes restricting email to within the school, within the district, or not restricted.

Students should use their GWFE account for school work, not for their personal use and correspondence. In addition, students are advised to be careful and purposeful when sharing access to their documents with others, something that GWFE services makes easy to do in order to help students and teachers collaborate on projects.

When a student withdraws from the district or graduates, access to their student email account and related data in GWFE will be deactivated. Graduates will have the opportunity to download their Google data for a specified period of time following graduation.

Parents must grant their permission in order for a student to be issued a GWFE account. The parent's signature on the Student Handbook Acknowledgement Form will be considered as granting this permission. Parents who do not wish their child to be issued a GWFE account must submit a Restriction Letter to the school (see Parental Right to Restrict).

The Children's Online Privacy Protection Act (COPPA) applies to commercial companies and limits their ability to collect personal information from children under 13. Google's privacy policies assure school districts that regardless of the student's age it does not use GWFE services to collect or use student data for advertising purposes or to create advertising profiles. Ads are not displayed to students when they use GWFE services. In addition, GWFE email is not scanned for advertising purposes, nor is the information stored in GWFE Drives collected or used for any advertising purposes. Google has signed the K-12 School Service Provider Pledge to Safeguard Student Privacy. More information about Google Apps for Education and privacy can be found at http://www.google.com/edu/privacy.html.

Under the Family Educational Rights and Privacy Act (FERPA) and corresponding Alabama law, a student's *educational records*, excluding 'directory information', are protected from disclosure to third parties. The following 'directory information' will be uploaded to the LCS GWFE domain in order to create individual student accounts: student name, grade, school, and a password. Once a student begins using their account they may create *educational records* using GWFE services, for instance using Google's web-based tools to write papers or submit assignments for which grades may be given. Because Google will host these documents within the LCS GWFE domain, Google will be considered a "School Official" (as that term is used in FERPA and its implementing regulations). This means that Google will also comply with FERPA rules.

The general right of privacy will be extended to the extent possible in the electronic environment. However, Limestone County Schools cannot and does not guarantee the security of electronic files located on Google systems. The district applies content filtering and monitoring compliant with the Children's Internet Protection Act (CIPA) to all student accounts, and email is content filtered and encrypted by Google. However, no protection measures can be 100% effective. Therefore, the District cannot assure that the student will not be exposed to unsolicited information or that their account will never be compromised.

Parental Right to Restrict

Parents have the option of restricting certain activities related to technology use:

- Restrict a student under the age of 17 from independently using the Internet while at school
- Restrict a student account from being established on free, pre-approved websites when the websites require parental permission
- Restrict a student from being issued a Google Workspace for Education account

Opting out of a Google Workspace for Education account may significantly impair the student's ability to participate fully in the district's curriculum and educational program, as a school Google account is necessary to use district laptops and access essential digital educational tools.

Parents who wish to restrict a student's activities must notify the school in writing within five (5) days of the student's first day of attendance **each** school year. Students whose parents have notified the school that they want certain restrictions to be applied should abide by their parent's wishes in addition to all other rules in this Acceptable Use Agreement.

Permission to Use Technology
Students should only use technology with permission of a teacher, administrator, or other authorized school personnel. During school hours students should only use technology for school-related purposes. While in school, students must have specific permission from authorized school personnel in order to:

- Publish information to websites, blogs, wikis, messaging apps, or other online workspaces
- Create an account in any online software program or app

Additionally, students must have the permission of a school administrator and complete any necessary paperwork prior to removing any District-owned technology from the school.

Artificial Intelligence (AI)
Generative artificial intelligence (AI) is a new and emerging technology. As such, its uses and the implications of its use are still being discovered. For the purposes of the District's Technology Acceptable Use Agreement, it shall be treated as other established technologies. Students are prohibited from generating work with AI and claiming it as their own creation. Any work produced must be properly cited and/or attributed to the generative engine.

Rules and Limitations
Students should strive to be good 'digital citizens.' In addition to following this AUA, 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.

Examples of Unacceptable Use

This list is not all-inclusive but is intended to provide general guidance. Anything that would be considered inappropriate in "paper form" or "verbal form" is also considered inappropriate in electronic form. Information, such as but not limited to Student Information System (SIS) data, accessed through school system technologies may not be used for any private business activity. Students may be held responsible for other inappropriate actions whether or not they are specifically included in this AUA. The following are examples of inappropriate activities when using any Limestone County Schools' network, email system, hardware, software, technology services, and/or internet access.

Students shall not tamper, disable, damage, or disrupt technology systems and resources:

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.
6. Intentionally damage, delete, destroy, or interrupt access to software or data 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 permission from authorized school personnel.
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.

Students shall not invade, trespass, spy, falsify, cheat, waste, or use technology resources:

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 assist 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.

Students shall not 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.

Students shall not 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.