[redacted]

ACCEPTABLE USE PRACTICE (AUP) RULES AND REGULATIONS

Technology

SCBOE 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 may 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 District-owned or managed technology regardless of location or time of day.

Online Accounts & COPPA

Throughout the year, teachers may wish for their students to use free or paid, educationally appropriate websites or apps, some of which will require that each student have an individual user account. In order to create such accounts, the District may upload certain 'directory information' (see FERPA) to the provider, generally the student's name, school, and grade level. SCBOE will review the privacy policies of such websites in advance of their use. For a list of reviewed sites, visit http://www.shelbyed.k12.al.us/tech/stu_web_acct.html.

In compliance with the Children's Online Privacy Protection Act (COPPA) of 1998, any person under the age of 13 must receive explicit parental permission in order to sign up for any online service where their personal information may be shared, unless that person is part of a subscribing school that provides COPPA consent on behalf of parents. SCBOE will provide such consent on behalf of parents unless the parent properly notifies the school that they deny such permission. Parents who may wish to opt out of this permission should first speak to their child's school so that they understand the impact this may have on the digital tools available to their child. If the parent still wishes to opt out, instructions on how to do so are found in the *Parent Notifications and Parent's Right to Restrict* portion of this Code of Conduct.

Parental Right to Restrict

Parents have the option of restricting certain activities related to technology use. For complete information and directions on how to notify the school about any of the following restrictions, see the "Parental Notifications" section later in this Code of Conduct.

- 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 (grades K-12) from being issued a Google Apps for Education account

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 Policy.

Personally-Owned Technology

As part of the District's Bring Your Own Device (BYOD) program, some schools allow students to bring their own devices to school for educational use. 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. Devices and rules may vary from school to school.

Students must first determine if their school has a BYOD program and, if so, which devices are allowed. Before bringing a device to school, the student should get their parent's permission to do so. The following devices may not be brought to school:

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

Students may only use personal technology during school hours when given specific permission to do so by their teacher or a school administrator.

Students must also follow all rules established by the transportation department regarding the use and storage of personal devices while on the 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 when the student has not properly secured it.

In addition to any other applicable consequences, students who are found to have used their personal device at school in manner that violates any section of the Shelby County Schools Code of Conduct, including this Acceptable Use Policy, **may lose the privilege to bring their personal device to school either temporarily or permanently**. This includes:

- Use of a personal device to access inappropriate content, not limited to content that would be blocked by the District's Internet filter. This includes content that may be stored on the device itself.

- Use of the device to capture video, images, or audio in areas of the school where others have an expectation of privacy. These include, but are not limited to locker rooms, restrooms, etc.

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.

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 AUP 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.

Permission to Use Technology

In general, students should only use technology with permission of a teacher or administrator. The school's BYOD policy will determine when and how students may use personally-owned devices. During school hours students should only use technology, whether the District's or their own, for school-related purposes. While in school, students must have specific permission from their teacher in order to:

- Use personally-owned technology in class
- Publish information to websites, blogs, wikis, messaging apps, or other online workspaces, including Twitter
- 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.

Unauthorized Video/Audio Recording

1. The Board of Education values civility, respect for the individual and the privacy of students, visitors and staff. These values include safeguarding against inappropriate invasions of personal privacy rights. In addition to the privacy protections provided by applicable laws and regulations, other policies of the Board of Education, and reasonable regulations promulgated by building and central administrators, the following guidelines shall apply to photographs, video recordings and audio recordings on School District premises.
2. Except as specifically set forth in these guidelines, no person present on School District premises shall make, publish or distribute any photograph, video recording or audio recording (collectively, "Recordings") capturing the image or voice of any other person on School District premises (a "Recording Subject") without the express prior permission of the Recording Subject. Violation of these guidelines shall be subject to the following potential consequences:
   (a) In the case of violations by staff, disciplinary action as permitted by law and subject to the terms of any applicable collective bargaining agreement;
   (b) In the case of violations by students, (i) confiscation of recording equipment until any unauthorized Recording has been erased, and (ii) disciplinary action pursuant to the School District's Code of Conduct;
   (c) In the case of visitors, ejection from School District premises and other appropriate action.
3. The following Recordings may be made <u>without</u> the prior consent of a Recording Subject, subject to any further privacy protections provided by applicable laws and regulations, and *provided*, *further*, that no otherwise-permitted Recording shall be distributed or disseminated for the purpose of annoying, intimidating or harassing any Recording Subject:
   (a) Recordings made by or on behalf of the School District for inclusion in School District publications and newsletters or for dissemination to the news media for the purpose of publicizing School District programs or events.
   (b) Recordings made by representatives of news media, parents and other persons lawfully on School District premises to attend School District events open to visitors, including dramatic productions, athletic events, meetings of the Board of Education and other meetings open to the public on School District premises; *provided*, *however*, that Recordings may be limited in the case of performances of copyrighted material.
   (c) Recordings made in connection with certification and other credentialing processes applicable to teachers and teaching assistants.
   (d) Recordings made with the approval of the Superintendent of Schools for the purpose of assessing or improving the quality of instruction.
   (e) Recordings made by faculty members for educational purposes tied to the goals and objectives of a course or courses, or for dissemination only in the faculty member's password protected site.
   (f) Recordings made for use in connection with class photographs, student publications and yearbooks.
   (g) Recordings made and maintained by the School District for security purposes.

(h) Recordings of interior or exterior scenes where the presence of Recording Subjects who have not given consent is merely part of an incidental background.

(i) Such other Recordings as are approved in advance by the Superintendent of Schools, the Assistant Superintendent of Schools or a Building Principal, which approval may include appropriate restrictions.

G-Suite for Education Services (Formerly called Google Apps for Education)

As part of its technology services, SCBOE will provide students in grades K-12 with a G-Suite for Education account. G-Suite accounts give students access to certain core Google services in an environment managed by the school district. SCBOE will issue all G-Suite accounts and manage which features will be made available to students. The core G-Suite for Education services that will be made available to students include Google Docs and Google Drive, used for creating and storing documents. Additional tools built into these products will assist students in conducting and documenting research, collaborating with others, and submitting work to teachers. As part of the G-Suite for Education core services, students will also receive a District-controlled email account and calendar for school use. The District may restrict email to within the school, within the district, or not restricted. Parents will have the ability to view their child's account.

Students should use their G-Suite 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 G-Suite services makes easy to do in order to help students and teachers collaborate on projects.

Parents must grant their permission in order for a student to be issued a G-Suite account. The parent's signature on the school's Code of Conduct acknowledgement form will be considered as granting this permission. Parents who do not wish their child to be issued a G-Suite account must submit a Restriction Letter to the school within 5 days of their student's first day of school. It is strongly recommended that parents who are considering this restriction contact their child's school first so that they fully understand how such denial will impact what digital tools their child may access. Directions for submitting the Restriction Letter are found in the "Parental Notifications" section of this Code of Conduct.

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 G-Suite for Education core services to collect or use student data for advertising purposes or to create advertising profiles. Ads are not displayed to students when they use the District's G-Suite for Education core services, nor is any student content scanned for advertising purposes. Google has signed the K-12 School Service Provider Pledge to Safeguard Student Privacy (http://studentprivacypledge.org/?page_id=45). More information about G-Suite 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 SCBOE G-Suite 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 G-Suite 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 District's G-Suite 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, SCBOE cannot and does not guarantee the security of electronic files located on Google systems. Google does apply a powerful content filter for email. 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 hacked.

Parents who do not agree to these terms must properly notify their child's school by following the directions in the "Notifications to Parents" section of this Code of Conduct within 5 days of their student's first day of school.

Examples of Unacceptable Use

The following 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 Board-owned or managed networks.
12. Install or modify wireless connectivity devices such as wireless access points and routers.
13. Connect personal devices to Board-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 invade, trespass, spy, falsify, cheat, waste, or use technology resources for personal purposes ...

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, 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 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 Board technology or 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; sent via email, text or any other message sharing technology; or stored on any device. This applies even when the service or device being used is personally-owned.
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.
40. Use or access any anonymizing or disappearing messaging apps or programs for any purpose.

Students shall not use Technology to compromise the personal privacy, reputation, identity, or safety of themselves or others ...

41. Attempt to read, delete, copy, forward, or modify email or electronic files of others.
42. Post any false or damaging information about other people, the school system, or other organizations.
43. Falsely post as an employee of the Board of Education on any website, online forum, social networking site, or other online venue.
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 district-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 *Shelby County Board of Education Student Code of Conduct and Attendance*. 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 SCBOE 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 provided by the school, students and parents affirm that they have received and understand these rules and regulations. However, failure to sign or return a signed form does not release students from their obligation to abide by these rules and regulations and all other applicable Board policies.

[redacted]