Trussville City Schools
Responsible Use of Technology for Students

Trussville City Schools makes a variety of communications and information technologies available to students through computer/network/Internet access. These technologies, when properly used, promote educational excellence in Trussville City Schools by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the Trussville City Schools, its students and its employees. The Responsible Use Guidelines are intended to minimize the likelihood of such harm by educating students and setting standards which will serve to protect. Trussville City Schools firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

Mandatory Review

To educate students on proper computer/network/Internet use and conduct, students are required to review these guidelines at the beginning of each school year. All students shall be required to acknowledge receipt and understanding of all guidelines governing use of the system. The parent or legal guardian of a student user is required to acknowledge receipt and understanding of the Responsible Use Guidelines of Technology for Students (hereinafter referred to as the Responsible Use Guidelines) as part of their review of the *Student Code of Conduct* handbook. Employees supervising students who use the District's system will provide training emphasizing its appropriate use.

Definition of TCS Technology System

The TCS's computer systems and networks (system) are any configuration of hardware and software. The system includes but is not limited to the following:

- Telephones, cellular telephones, and voicemail technologies;
- Email accounts;
- Servers;
- Computer hardware and peripherals;
- Software including operating system software and application software;
- Digitized information including stored text, data files, email, digital images, and video and audio files;
- Internally or externally accessed databases, applications, or tools (Internet- or Board-server based);
- Board-provided Internet access;
- Board-filtered public Wi-Fi;
- Virtual environments; and
- New technologies as they become available.

Availability of Access

Acceptable Use

Computer/Network/Internet access will be used to enhance learning consistent with the District's educational goals. The Board requires legal, ethical and appropriate computer/network/Internet use by all students.

Privilege

Access to the Board's computer/network/Internet is a privilege, not a right. Persons who violate any Board policy, rule, or procedure regarding technology use may be denied use of the Board's technology resources and may be subject to additional disciplinary action. (**Restriction or Loss of Technology Privileges, Board Policy 4.92**)

Access to Computer/Network/Internet

The Board permits restricted and conditional access to and use of its technology resources, including but not limited to computers, the "Internet," and network storage areas. Such access and use is restricted to employees, students, and other persons who are engage in bona fide educational and administrative activities that serve and are consistent with identified educational objectives or authorized support functions, and who, by signing the Responsible Use of Technology for Students, agree to abide by all Board policies, rules, and regulations regarding technology use. Each Board computer and public Wi-Fi (available for students who bring their own personal devices) utilizes filtered Internet access as defined by Children's Internet Protection Act.

- Students should NOT attempt to install software or hardware or change the system configuration including network settings without prior consultation with Tech Support.
- Students are expected to protect school devices from damage and theft.
- Students could be monetarily responsible for any hardware damage that occurs off school premises and/or software damage (including labor costs). This includes replacement of equipment at comparable replacement cost.
- Students will not be held responsible for computer problems resulting from regular school-related use; however, students may be held personally responsible for any problems caused by their negligence as deemed by the District's administration.
- Students will provide access to any device, equipment, and/or accessories they have been assigned upon the District's request.
- Students are required to maintain password confidentiality by not sharing their password with others and may not use another person's system account. (Appendix H Password Control Standards, Data Governance Procedures, Policy I 15.2)
- Students identified as a security risk or having violated the Board's Responsible Use of Technology for Students may be denied access to the Board's system. Other consequences may also be assigned.

Student Access

Computer/Network/Internet access is provided to all students unless parents or guardians denied access during online registration. Student Internet access will be under the direction and guidance of a Board staff member. Students may also be allowed to use the local network and public Wi-Fi with campus permission.

Students 13 or Younger

As part of our instructional programs, the Board registers students on a number of educational websites. The Children's Online Privacy Protection Act (COPPA) requires additional parental permission to register students under 13 years old on these educational websites. The information provided to these websites is basic "directory information." Typically, this is the student's name, grade and school. Examples of these tools are Google Applications for Education, Google Classroom, Raz Kids, online textbooks, Accelerated Reading, etc. These tools can be accessed through the school's student resource page. Parents wishing to deny access to these educational tools must do so in writing to the campus principal indicating their child should be denied access to these tools.

Use of Personal Devices

The Board believes technology is a powerful tool that enhances learning and enables students to access a vast amount of academic resources. The Board's goal is to increase student access to digital tools and facilitate immediate access to technology-based information, much the way that students utilize pen and paper. To this end, the Board offers a filtered, wireless network through which students have the ability to connect privately owned (personal) devices. Students are allowed to bring personal devices connected to the Trussville City Schools network for academic classroom use as determined by the classroom teacher. Each campus will develop procedures for use and management.

Security

A student who gains access to any inappropriate or harmful material is expected to discontinue the access and to report the incident to the supervising staff member. Any student identified as a security risk or as having violated the Responsible Use Guidelines may be denied access to the Board's system. Other consequences may also be assigned. A student who knowingly brings prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the Board's system and will be subject to disciplinary action in accordance with the Board-approved *Student Code of Conduct*.

Subject to Monitoring

All technology resources, including network and Internet resources, e-mail systems, and computers or other devices owned, leased, or maintained by the Board are the sole property of the Board. Board personnel may, at any time and without prior notice, access, search, examine, inspect, collect, or retrieve information of any kind from the Board's technology resources, including computer or related equipment, files, and data, to determine if a user is in violation of any of the Board's policies, rules, and regulations regarding access to and use of technology resources, for or in connection with any other matter or reason related to the safe and efficient operation or administration of the school system, or for any other reason not prohibited by law. Users of school system technology resources have no personal right of privacy or confidentiality with respect to the use or content of such resources. (**Ownership of Technology Resources and Data, Board Policy 4.93**)

Student Computer/Network/Internet Responsibilities

Board students are bound by all portions of the Responsible Use Guidelines. A student who knowingly violates any portion of the Responsible Use Guidelines will be subject to suspension of access and/or revocation of privileges on the Board's system and will be subject to disciplinary action in accordance with the Board-approved *Student Code of Conduct*.

Use of Digital Tools

Students may participate in Board-approved online learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, Google Drive, online meeting sessions, etc. The use of blogs and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of Board-approved digital tools. Digitally transmitted content that includes inappropriate language, images or content is prohibited.

Password Confidentiality

Students are required to maintain password confidentiality by not sharing their password with others. Students may not use another person's system account.

Reporting Security Problem

If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the student should immediately notify the supervising staff member. The security problem should not be shared with others.

The following guidelines must be adhered to by students using a personally-owned device at school:

- If network access is needed, students must connect to the filtered, wireless network provided by the Board, TCS Student.
- These devices are the sole responsibility of the student owner. The school or Board assumes no responsibility for personal devices if they are lost, loaned, damaged or stolen and only limited time or resources will be spent trying to locate stolen or lost items.
- These devices have educational and monetary value. Students are prohibited from trading or selling these items to other students on Board property, including school buses, and at school-sponsored or school-related activities on or off school property.
- Each student is responsible for his/her own device: set-up, maintenance, charging, and security. Staff members will not store student devices at any time, nor will any Board staff diagnose, repair, or work on a student's personal device.
- Availability of devices will not be used as a factor in grading or assessing student work. Students who do not have access to personal devices will be provided with comparable Board-owned equipment or given similar assignments that do not require access to electronic devices.
- Devices are only to be used for educational purposes at the direction of a classroom teacher or as stated for specific age groups.
- School administrators or their designees have the authority to restrict and deny the use of personal, wireless communication devices by any student to prevent the misuse, abuse, or violation of school rules regarding the use of such devices. School officials may read, examine, or inspect the contents of any such device upon reasonable suspicion that the device contains evidence of a violation of law, Board policy, the Code of Student Conduct, or other rules, provided that the nature and extent of such examination shall be reasonably related and limited to the suspected violation.
  [Reference: ALA. CODE §16-1-27 (1975)]

Inappropriate Use

Inappropriate use includes, but is not limited to, those uses that violate the law, that are specifically named as violations in this document, that violate the rules of network etiquette, or that hamper the integrity or security of this computer/network/Internet system or any components that are connected to it. The following actions are considered inappropriate uses, are prohibited, and will result in revocation of the student's access to the computer/network/Internet.

Violations of Law

Transmission of any material in violation of any federal or state law is prohibited. This includes, but is not limited to:

- threatening, harassing, defamatory or obscene material;
- copyrighted material;
- plagiarized material;
- material protected by trade secret; or
- blog posts, Web posts, or discussion forum/replies posted to the Internet which violate federal or state law.

Tampering with or theft of components from Board systems may be regarded as criminal activity under applicable state and federal laws. Any attempt to break the law through the use of a Board computer/network/Internet account may result in prosecution against the offender by the proper authorities. If such an event should occur, the Board will fully comply with the authorities to provide any information necessary for legal action.

Modification of Computer

Modifying or changing computer settings and/or internal or external configurations without appropriate permission is prohibited.

Transmitting Confidential Information

Students may not redistribute or forward confidential information without proper authorization. Confidential information should never be transmitted, redistributed or forwarded to outside individuals who are not expressly authorized to receive the information. Revealing personal information (such as, but not limited to, home addresses, phone numbers, email addresses, birthdates) about oneself or of others is prohibited.

Commercial Use

Use of the system for any type of income-generating activity is prohibited. Advertising the sale of products, whether commercial or personal is prohibited.

Marketing by Non-TCS Organizations

Use of the system for promoting activities or events for individuals or organizations not directly affiliated with or sanctioned by the Board is prohibited.

Vandalism/Mischief

Any malicious attempt to harm or destroy Board equipment, materials or data~~,~~ or the malicious attempt to harm or destroy data of another user of the Board's system, or any of the agencies or other networks to which the Board has access is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of Board policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above is prohibited and will result in the cancellation of system use privileges. Students committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences. [See the Board-approved *Student Code of Conduct*.]

Intellectual Property/Copyright Violations

Students must always respect copyrights and trademarks of third-parties and their ownership claims in images, text, video and audio material, software, information and inventions. The copy, use, or transfer of others' materials without appropriate authorization is not allowed. Downloading or using copyrighted information without following approved Board procedures is also prohibited.

Plagiarism

Fraudulently altering or copying documents or files authored by another individual is prohibited.

Impersonation

Attempts to log on to the computer/network/Internet impersonating a system administrator or Board employee, student, or individual other than oneself, will result in revocation of the student's access to computer/network/Internet.

Illegally Accessing or Hacking Violations

Intentional or unauthorized access or attempted access of any portion of the Board's computer systems, networks, or private databases to view, obtain, manipulate, or transmit information, programs, or codes is prohibited.

File/Data Violations

Deleting, examining, copying, or modifying files and/or data belonging to other users, without their permission is prohibited.

System Interference/Alteration

Deliberate attempts to exceed, evade or change resource quotas are prohibited. The deliberate causing of network congestion through mass consumption of system resources is prohibited.

Email and Communication Tools

Email and other digital tools such as, but not limited to Google Apps for Education, blogs and online resources, are tools used to communicate within the Board. The use of these communication tools should be limited to instructional or school-related activities. Email is subject to monitoring by appropriate staff.

Students should keep the following points in mind:

Perceived Representation

Using school-related email addresses and other communication tools might cause some recipients or other readers of the email to assume that the student's comments represent the Board or school, whether or not that was the student's intention.

Privacy

Email, Google Apps for Education, and other communication within these tools should not be considered a private, personal form of communication. Private information, such as home addresses, phone numbers, last names, pictures, or email addresses, should not be divulged.

Inappropriate Language

Using obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language in emails or other communication tools is prohibited. Sending messages that could cause danger or disruption, personal attacks, including prejudicial or discriminatory attacks are prohibited.

Forgery

Forgery or attempted forgery of email messages is prohibited. Attempts to read, delete, copy or modify the email of other system users, deliberate interference with the ability of other system users to send/receive email, or the use of another person's user ID and/or password is prohibited.

Junk Mail/Chain Letters

Students should refrain from forwarding emails which do not relate to the educational purposes of the Board. Chain letters or other emails intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any annoying or unnecessary message to a large number of people (spamming) is also prohibited.

Student Email Accounts and Electronic Communication Tools

Electronic communication is an important skill for 21st Century students. By providing this tool, the Board is equipping students with the skills necessary for success in the business. Students in grades 3 - 12 are given access to a Board student email account. This account is set up with the student's user ID. Students must abide by the guidelines established within Email and Communication Tools. Student email accounts will be available for use by students in grades 3-12 while they are currently enrolled in the Board. As appropriate, project email accounts may be granted for educational activities for students in grades K-2 at the request of the classroom teacher.

Consequences of Agreement Violation

Any attempt to violate the provisions of this agreement may result in revocation of the student's access to the computer/network/Internet, regardless of the success or failure of the attempt. In addition, school disciplinary and/or appropriate legal action may be taken.

Denial, Revocation, or Suspension of Access Privileges

With just cause, the building principal or Technology Coordinator, may deny, revoke, or suspend computer/network/Internet access as required, pending an investigation.

Warning

Sites accessible via the computer/network/Internet may contain material that is illegal, defamatory, inaccurate or controversial. Each Board computer with Internet access has software that utilizes filtered Internet access as defined by Children's Internet Protection Act. The Board makes every effort to limit access to objectionable material; however, controlling all such materials on the computer/network/Internet is impossible, even with filtering in place. With global access to computers and people, a risk exists that students may access material that may not be of educational value in the school setting.

Limitation on Liability

The Board makes no warranties of any kind either express or implied, that the functions or the services provided by or through the Board's technology resources will be error-free or without defect. The Board will not be responsible for damage users may suffer, including but not limited to loss of data or interruption of services. (**Board Policy 4.95**)
[Reference: 47 U.S.C. 254(h) and (l)]