Trussville City Schools
Responsible Use of Technology for Staff

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

Mandatory Review

To educate staff on proper computer/network/Internet use and conduct, users are required to review these procedures at the beginning of each school year. All staff shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system. These procedures are included in the Trussville City Schools' Faculty and Staff Handbook.

Definition of Board Technology System

The Board'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
- Fax machines
- Copiers
- 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, 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 improve teaching and enhance learning consistent with the Board's educational goals. The Board requires legal, ethical and appropriate computer/network/Internet use by all Board staff.

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," network storage areas, and electronic mail. 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 a Staff or Student Responsible Use Procedure for Technology agreement, agree to abide by all Board policies, rules, and regulations regarding technology use. The Responsible Use of Technology for Staff or Student agreement will be developed by the Superintendent for approval by the Board. (**Access to Technology Resources, Board Policy 4.91**) All such agreements will be maintained on file in the Technology Department.

- Staff members should NOT attempt to install software or hardware or change the system configuration including network settings without prior consultation with Tech Support.
- Staff members are expected to protect school laptops from damage and theft.
- Each staff member is 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.
- Staff members will not be held responsible for computer problems resulting from regular school-related use; however, staff members will be held personally responsible for any problems caused by their negligence as deemed the District's administration.
- Staff members will provide access to any laptop computer, equipment, and/or accessories they have been assigned upon the District's request.
- Staff 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)
- Staff identified as a security risk or having violated the Board's Staff Responsible Use Procedures may be denied access to the Board's system. Other consequences may also be assigned.
- Computer/Network/Internet access is provided to all Board staff.
- Each Board computer and public Wi-Fi (available for individuals who bring their own personal telecommunication devices) has software installed that utilizes filtered Internet access as defined by Children's Internet Protection Act.
- Limited personal use is permitted if the use imposes no tangible cost to the Board, does not unduly burden the Board's computer or network resources, and has no adverse effect on a staff member's job performance.
- All non-staff/non-student users must obtain approval from the principal, departmental supervisor and Technology Coordinator through a Work Order Request Form to gain individual access to the Board's system.

Content/Third-Party Supplied Information

Staff with access to the Board's system should be aware that use of the system may provide access to other electronic communication systems in the global electronic network that may contain inaccurate and/or objectionable material.

Staff who knowingly bring prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with Board policies.

Subject to Monitoring

All technology resources, including network and Internet resources, e-mail systems, and computers or other access 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**)

Use of Personal Devices

The Board will provide a filtered, wireless public network to which staff will be able to connect personal telecommunication devices for instructional and administrative functions. These devices are the sole responsibility of the staff owner. The school or Board assumes no responsibility for personal telecommunication 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. Each staff member is responsible for their own device; set up, maintenance, charging and security. Board staff will not diagnose, repair or install software on another staff members or student's device. Any and all school district information on the personal device is subject to examination, retrieval, search and/or subpoena.

Staff Computer/Network/Internet Responsibilities

Staff are responsible for their actions in accessing available resources.

Board staff are bound by all portions of the Board's Staff Responsible Use of Technology. Staff who knowingly violate any portion of the Responsible Use of Technology for Staff will be subject to disciplinary action in accordance with Board policies.

School and Departmental-Level Responsibilities

The principal/departmental administrator or designee will:

1. Be responsible for disseminating and enforcing the Board's Technology Policies and Responsible Use of Technology for Staff and Student at the school or departmental level such as unauthorized disclosure, use, and dissemination of personal information regarding minors; prevention of hacking or other forms of unauthorized use of or access to files, sites, databases or equipment, etc. (Board Policy 4.9)

2. Ensure that all staff users of the Board's system complete and sign an agreement to abide by Board policies and administrative regulations regarding such use. All such agreements will be maintained on file in the Technology Department's office.
3. Ensure that staff supervising students who use the Board's systems provide education and information emphasizing its appropriate, safe, and ethical use.
4. Monitor all users of the Board's systems to ensure appropriate and ethical use.
5. Use the Board's student information system to identify students who do not have permission to use the Internet and inform staff who are responsible for these students that they do not have permission to use the Internet, student email or Websites that require parental consent for students under the age of 13.
6. Provide training to staff that supervise students on digital responsibility, digital citizenship/ and appropriate use of technology resources.

Teacher Responsibilities

The teacher will:

1. Provide age-appropriate lessons in Internet safety, digital responsibility, and cyber security for students throughout the year.
2. Review Board computer/network/Internet responsibilities prior to gaining access to such system.
3. Verify the list of students (age 13 and younger) who require additional parent consent to access the Internet, email, and Websites through email received from office.
4. Provide developmentally-appropriate guidance to students as they use electronic resources related to instructional goals.
5. Use computer/network/Internet in support of instructional goals.
6. Provide alternate activities for students who do not have permission to use the Internet or email.
7. Provide a variety of comparable activities for students who do not bring their own device.
8. Address student violations of the Board's Responsible Use of Technology for Students as defined in the *Student Code of Conduct*.
9. Prevention unauthorized disclosure, use, and dissemination of personal information regarding minors to other persons including third party software companies. Approval must be obtained through submitting a Work Order Request Form (WORF) which will be reviewed by school and district data governance teams. (**Data Governance Policy, I 15.2 (4.10) and Procedures**)

Staff Code of Conduct

Board staff are expected to maintain appropriate conduct when accessing the communications and information technologies available through computer/network/ Internet access. All staff must comply with the Board's Responsible Use of Technology for Staff at all times when accessing any part of the technology system.

Staff will guard and protect access to secure systems by:

1. **Protecting passwords and other similar authorization information.** Passwords are the primary way in which staff members are authenticated and allowed to use the Board's computing resources. Staff will not disclose personal password(s) to any individual, including another staff member. Similarly, staff will not disclose other identifying information used to access specific system information, recognizing that if they do so, they will be held accountable for their actions as well as those of other parties to whom they have given access.
2. **Guarding unauthorized use of resources.** Staff will not allow others to make use of their accounts or network access privileges to gain access to resources to which they would otherwise be denied.
3. **Not circumventing or compromising security.** Staff must not utilize any hardware or software in an attempt to compromise the security of any other system, whether internal or external to the Board's systems and network. Examples of prohibited activities include (but are not limited to) Trojan horses,

password crackers, port security probes, network snoopers, IP spoofing, and intentional transmission of viruses or worms.

Computer/Network/Internet usage is subject to monitoring by designated staff at any time to ensure appropriate use. Electronic files sent, received or stored anywhere in the computer system are available for review by any authorized representative of the Board for any purpose. Staff will affirm, in writing that at all times their actions while using the Board's system will not violate the law or the rules of network etiquette, will conform to the Procedures set forth in the Staff Responsible Use Procedures, and will not violate or hamper the integrity or security of the Board's technology system.

If a violation of the Responsible Use of Technology for Staff occurs, staff will be subject to one or more of the following actions:

1. Revocation of access
2. Possible monetarily responsibility
3. Disciplinary action
4. Loss of employment with the Board
5. Appropriate legal action

Use of Online Tools and Resources

Communication with students and parents should be conducted through district issued website and email. It is recommended that any social media communication occur within the school's social media pages. See your administrator for more information regarding approval and process for publishing information through the school's social media pages.

The use of any online tool and resources is considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate online. Staff who use digital learning tools in their classrooms must monitor student actions to ensure compliance with *the Responsible Technology of Technology for Students in the Student Code of Conduct*.

Use of System Resources

Staff are asked to purge email or outdated files on a regular basis.

Reporting Security Problem

If knowledge of inappropriate material or a security problem on the computer/network/Internet is identified, the staff should immediately notify the Board's Help Desk at 3006. The security problem should not be shared with others.

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 and are prohibited:

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 the litigation process.

Modification of Computer

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

Transmitting Confidential Information

Staff may not redistribute or forward confidential information (i.e. educational records, directory information, personnel records, etc.) 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 about oneself such as, but not limited to, home addresses, phone numbers, email addresses, birthdates of or of others is prohibited. (Data Governance and Use Policy, I 15.2 (4.10)

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. Staff committing vandalism will be required to provide restitution for costs associated with system restoration and may be subject to other appropriate consequences.

Copyright

Staff 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. "Over the years, librarians, educators, and publishers have developed voluntary guidelines to address fair use," Willard told Education World. "Although these guidelines are not statutory, they are contained in the legislative history of the Copyright Act."

Those guidelines **allow** educators, under most circumstances, to copy or use

- a single chapter from a book
- an excerpt from a work that combines language and illustrations, such as a children's book, not exceeding two pages or 10 percent of the work, whichever is less
- a poem of 250 words or less or up to 250 words of a longer poem
- an article, short story, or essay of 2,500 words or less, or excerpts of up to 1,000 words or 10 percent of a longer work, whichever is less; or
- a single chart, graph, diagram, drawing, cartoon, or picture from a book, periodical, or newspaper.
- up to three minutes or 10 percent, whichever is less, of a single copyrighted motion media work
- up to 30 seconds or 10 percent, whichever is less, of music and lyrics from a single musical work
- up to five photographs or illustrations by one person and no more than 15 images or 10 percent, whichever is less, of the photographs or illustrations from a single published work
- up to 2,500 fields or cell entries or 10 percent, whichever is less, from a numerical database or data table
- all multimedia projects that include copyrighted materials credit the sources, display the copyright notice, and provide copyright ownership information. (The credit identifies the source of the work, including the author, title, publisher, and place and date of publication. The copyright ownership information includes the copyright notice, year of first publication, and name of the copyright holder.)

The guidelines **do not** allow users to

- make multiple copies of different works as a substitute for the purchase of books or periodicals
- copy the same works for more than one semester, class, or course
- copy the same work more than nine times in a single semester
- use copyrighted work for commercial purposes
- use copyrighted work for over two years without obtaining permission
- use copyrighted work without attributing the author.

- See more at: http://www.educationworld.com/a_curr/curr280b.shtml#sthash.nmh5JpmW.dpuf

Copyright Violations
Downloading or using copyrighted information without following approved Board procedures is prohibited.

Intellectual Property
An original work created by a student that will be published on the Internet will require written parental consent.

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 staff, student, or individual other than oneself, will result in revocation of the staff member'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 online learning environments, websites, blogs, and other online resources, are tools used to communicate within the Board. The use of these communication tools should be limited to instructional, school-related activities, or administrative needs. Employees must only use @trussvillecityschools.com, @tvboe.com, or @trussvillecityschools.org email addresses to create school related online accounts.

Communication with students and parents should be conducted through district issued website and email.

Staff will be issued email accounts. Staff should check email frequently, delete unwanted messages promptly, and stay within the email server space allocations. Email attachments, both internal and external, are limited to 50MB or smaller.

Staff should keep the following points in mind:

Perceived Representation

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

Privacy

Email, online learning environments, websites, blogs and other communication within online 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. To avoid disclosing email addresses that are protected, all email communications to multiple recipients should be sent using the blind carbon copy (bcc) feature, if applicable.

Inappropriate Language

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

Communications with Students

Communication with students and parents should be conducted through district issued website and email.

Employees shall refrain from inappropriate communication with a student or minor, including, but not limited to, electronic communication such as cell phone, text messaging, email, instant messaging, blogging, or other online communication tools. The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity). Communication should be within a group setting and not individual.

Factors that may be considered in assessing whether the communication is inappropriate include, but are not limited to:

- The nature, purpose, timing, and amount of the communication;
- The subject matter of the communication;
- Whether the communication was made openly or the educator attempted to conceal the communication;
- Whether the communication could be reasonably interpreted as soliciting sexual contact or a romantic relationship;
- Whether the communication was sexually explicit; and
- Whether the communication involved discussion(s) of the physical or sexual attractiveness or the sexual history, activities, preferences, or fantasies of either the educator or the student.

The employee does not have a right to privacy with respect to communications with students and parents.

The employee continues to be subject to federal laws, local policies, and administrative regulations, and the Alabama Code of Ethics including:

- Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records.
- Copyright law
- Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student.

Upon request from administration, an employee will provide the phone number(s), online site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with any one or more currently-enrolled students.

Political Lobbying

Consistent with State ethics laws, Board resources and equipment, including, but not limited to, emails, blogs or other communication tools must not be used to conduct any political activities, including political advertising or lobbying. This includes using Board email or other communication tools to create, distribute, forward, or reply to messages, from either internal or external sources, which expressly or implicitly support or oppose a candidate for nomination or election to either a public office or an office of a political party or support or oppose an officeholder, a political party, or a measure (a ballot proposition). These Procedures prohibit direct communications as well as the transmission or forwarding of emails, hyperlinks, or other external references within emails regarding any political advertising.

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

Staff should refrain from forwarding emails which do not relate to the educational purposes of the Board. Chain letters or other email intended for forwarding or distributing to others is prohibited. Creating, distributing or forwarding any unnecessary message to a large number of people (spamming) is also prohibited. Such emails should be deleted without opening.

Board and School Websites Responsibilities

The purpose of Board websites is to communicate Board, school and/or class activities and information. Official school and Board Web sites should be hosted on a Board provided site.

The principal and or Board reserves the right to alter or delete any content contained on a Board Web site in order to ensure that it conforms with the school and Board's communications objectives.

Content Issues

For the requirements below, "content" is defined as text, graphics, media, or other information that is visible and/or audible on a Board Web page.

Content shall not be displayed if it:

- ❖ Contains questionable and/or inappropriate material and/or themes.
- ❖ Is of a personal nature.
- ❖ Includes commercial, trademarked, and/or copyrighted material without the express written consent of the "owner" of the content. If consent is obtained, the proper trademark/copyright symbol and/or owner's credits must be displayed.
- ❖ Is out-of-date or inaccurate.
- ❖ Contains hyperlinks that do not return an active Web page and displays a "Page Not Found".
- ❖ Contains hyperlinks that do not return a document and displays a "Page Not Found".

Display of Student Information on the Internet

The following conditions apply to the display of student information on school and Board websites.

- Student-created projects, writings, and/or artwork are permitted on school/Board websites, or Board-approved blog and online sites, if the appropriate parental consent has been obtained.
- Student photographs and names are permitted only if the parent has given consent
- First name and last name initials should only be used

Consequences of Agreement Violation

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

Denial, Revocation, or Suspension of Access Privileges

With just cause, the building principal or Board 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 installed 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)]

I have read and understand the Responsible Use of Technology for Staff.

_____ _

Printed Name

_____ _____

Signature Date

_____

School