TECHNOLOGY ACCEPTABLE USE POLICY 5.90

PURPOSE:
The purpose of the Tuscaloosa County School System is to provide an effective, challenging, and engaging education for all students.

POLICY STATEMENT:
The primary goal of the technology environment is to support the educational and instructional endeavors of students and employees of Tuscaloosa County School System. Use of any and all technology resources is a privilege and not a right.

INTRODUCTION:
To ensure that students receive a quality education and that employees are able to work in a professional and intellectually stimulating environment, it is the policy of the Tuscaloosa County School System to provide all students and employees with access to a variety of technology resources. All Tuscaloosa County students and staff must acknowledge and adhere to this policy. The creation of a large and varied technology environment demands that technology usage be conducted in legally and ethically appropriate ways consistent with the Purpose Statement and instructional goals of the Tuscaloosa County School System. We recognize that the use of technology always requires attempts to balance the benefits against the possibilities of danger, security problems, and abuse. Rapid changes in technology and growth in the range of content available makes this balance a constant challenge.

Thus, it is the intention of the Tuscaloosa County School System that all technology resources be used in accordance with any and all school system policies and procedures as well as local, state, and federal laws and/or guidelines governing the usage of technology and its component parts. Additionally, it is implied that all students and employees of the Tuscaloosa County School System will use the provided technology resources so as not to waste them, abuse them, or interfere with or cause harm to other individuals, institutions, or companies. The administrators of each school are responsible for establishing specific practices to enforce this policy at individual schools.

Aspects of this policy may specifically address technology equipment personally owned by school system employees and/or students and brought into school facilities or onto school campuses to access school resources and/or personal resources. All personal technologies used on any Tuscaloosa County campus are subject to this policy and may be used only if such usage is in compliance with all school system policies, procedures, and guidelines as well as local, state, and federal laws. No technologies may be purchased, brought on campus, or used to access school system resources that interfere with or adversely affect functions or operations of school system technology resources or infrastructure.

All electronic content stored on any external storage medium or personal off-site storage location that is brought to or accessed from a Tuscaloosa County campus is subject to all school system policies and guidelines as well as local, state, and federal laws. Any questions about this policy, its interpretation, or specific circumstances shall be directed to the Director of Technology before proceeding. Violations of this policy will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action.

The Tuscaloosa County School System Technology Department issues further specific guidelines detailing appropriate and legal use of copyright, email, technology resource purchasing and disposal, web page creation and maintenance, and the publication of student work. These guidelines are updated as best practices dictate and as case law emerges. These guidelines are considered appendices of the Tuscaloosa County School System Technology Usage Policy. Students and staff are expected to be aware of and follow the guidelines that are updated as needed and posted on the Tuscaloosa County School System web site Board Policies section and on the Technology page and referenced in the Employee Handbook, Parent Student Information Guide and/or the Student Code of Conduct.

I. ACCESS and USAGE:

A. The use of all Tuscaloosa County School System technology resources is a privilege not a right, and inappropriate or suspected inappropriate use will result in a cancellation of those privileges pending investigation. Moreover, users of Tuscaloosa County School System technology must be aware that the Tuscaloosa County School System cannot assume any liability arising from the illegal or inappropriate use of technology resources.

B. Users should not purchase or dispose of software, hardware, peripherals, or other technology-related devices without consulting the technology staff. Regardless of purchase date, location, or funding source, all personnel should adhere to the Electronic Purchases and Disposal Guidelines of this policy.

C. Individuals may use only accounts, files, software, and/or other technology resources that are assigned to, provided for, or approved for him/her.

D. Individuals identified as a real or suspected security risk will be denied access.

E. Any use of technology resources, regardless of ownership, that reduces the efficiency of use for others will be considered a violation of this policy.

F. Employees/Students are prohibited from connecting any type of router, wireless Wi-Fi controller, bridging device or non-approved network switch to the local area or wide area network. Employees/Students are prohibited from establishing any private wireless or cabled local area network without obtaining written permission from the Information Technology Department. Any devices that are discovered will be confiscated by the Technology Department and at the discretion of the Director of Technology may or may not be returned to the personal owner. The system considers these types of devices as a possible security breach.

G. Individuals must not attempt to disrupt any technology services or data integrity by engaging in inappropriate activities. Examples include but are not limited to spreading viruses, spamming, excessive network and/or Internet activity, or modification of equipment or infrastructure.

H. Individuals must not attempt to modify technology resources, utilities, and configurations, and/or change the restrictions associated with his/her accounts, or attempt to breach any technology resource's security system or filtering systems, either with or without malicious intent. This includes proxy by-pass or redirect sites.

I. Bring Your Own Device (BYOD)/Personal technology-related devices such as but not limited to laptops, cell phones, smart-phones, iTouch/iPods/iPads/slate or tablet devices, cameras or other electronic devices, etc., used on school grounds are subject to all items covered in this policy and other applicable published guidelines. The permission for such personal devices to

be brought to school and the use of such devices will be at the discretion of the local school administrators and school rules. The user should not directly connect to school's local area network or wide area network resources that require authentication without the explicit permission from the Director of Technology. Student/Employee open access Internet connectivity for BYOD and visiting devices are subject to the conditions outlined in this policy and all other school system policies and guidelines as well as local, state, and federal laws. Students/Employees will be required to register their personal devices before obtaining access rights to these resources. Guest presenters will be provided access through the local school administrators and system technology staff. Due to the ability of broadband technologies that may reside in some of these personal devices (Smart-phones, MIFI, 3G-4G and future technologies), the system has no means to monitor the use or sites accessed from these devices while on school property. Users are responsible for proper conduct when using this form of technology communication at school or work. The board of education, school system, schools and employees of the system assume no responsibility or liability for the theft, loss, or damage to any personal devices or the inappropriate and/or misconduct use of an individual's device using non-system provided broadband or Wi-Fi connectivity. The system does not require students or employees to bring their own devices to school; however, we do believe such devices do provide students and teachers a resource tool that aids them in their education and job. During Testing all students must comply with the applicable procedures and guidelines established by the Assessment Department of the Alabama State Department of Education, ACT, College Board and/or system. Please see DIGITAL DEVICE POLICY IN A STANDARDIZED TEST SETTING in this policy and/or the Parent Student Information Guide. The system strongly advises all students not to bring cellular or other electronic devices on the campus or the testing location during the administration of standardized test.

J. Employees/Students are prohibited from sending/storing/saving on external storage, portable devices, and/or online cloud-based hosted storage sites such as but not limited to (Google Docs, Dropbox, etc.) that do not remain on campus or are approved by the Technology Department and/or approved by the Board of Education any classified data such as electronic copies of student or staff personal information, school or system documents. This information includes but is not limited to data containing social security numbers, student identification numbers, information protected by FERPA, and any other sensitive and/or protected information. In the event that this type of information is stored on a portable/external device or cloud based network and that device is lost or stolen, or if the security of this data is believed to have been breached in any way, the Director of Technology should be notified immediately.

K. The system Director of Technology and local school Administrator will determine when inappropriate use has occurred, and they have the right to deny, revoke, or suspend specific user accounts

II. PRIVACY:

A. To maintain network integrity and to ensure that the network is being used responsibly, if any policy violation or inappropriate behavior is suspected, the Director of Technology and local school Administrator reserve the right to inspect any and all communications/data activity,

including data stored by individual users on school devices. Users should be aware that activities may be monitored at any time without notice. In the event the suspected equipment is a personal device users may be asked to voluntarily allow system personnel the right to inspect their equipment. If permission is not granted and depending on the severity of the inappropriate use, a user's rights to bring the device on campus or system property may be denied or the system may elect to pursue legal or criminal action if warranted.

B. Users should not have any expectation that their use of technology resources, including user files stored on the Tuscaloosa County School System's network, will be private and will be secure from access by others. Reasonable steps will be taken to maintain the security of technology resources, but no assurance can be given that breach of such security will not occur.
C. Because communications on the Internet are public in nature, all users should be careful to maintain appropriate and responsible communications.
D. Tuscaloosa County School System cannot guarantee the privacy, security, or confidentiality of any information sent or received, via the Internet, email facility, telephone, or otherwise.
E. Users are encouraged to avoid storing personal and/or private information on the system and/or schools' technology resources.

III. DATA SECURITY:

A. Students and staff are expected to follow all local, state, and federal laws and system policy regarding the protection of student and staff confidential data.
B. Users should not have any expectation that their usage of such resources is private. Reasonable efforts will be taken to maintain security of technology resources, but the Tuscaloosa County School System cannot ensure that such security will not be breached and cannot assume any liability arising from any such breach of security.
C. Individuals must take all reasonable precautions to prevent unauthorized access to accounts and data and any other unauthorized usage within and outside the Tuscaloosa County School System. Any such unauthorized usage shall be reported immediately to the local school Administrator and/or the system Director of Technology of Technology.
D. All employees shall be responsible for reporting suspected or actual breaches of data security whether due to inappropriate actions, carelessness, loss/theft of devices, or failures of technical security measures.
E. Individuals may not attempt to log into the network using any network account and/or password other than the login(s) assigned to him/her. Individuals may not allow someone to use his/her network account and/or password to access the network, email, specific software packages, or the Internet.
F. Reasonable steps and procedures will be taken to secure student records, media center collections, child nutrition, and accounting information, and such information shall be backed up in a routine manner with such information being maintained in secure offsite or replicated storage location.
G. The system-wide technology staff does perform routine backups of critical systems and data in an effort to assure continuity of business. There can be no assurance, however, that technology resources will be available within a particular time frame after an outage. There is no guarantee that information that existed prior to an outage, malfunction, or deletion, can be recovered. Users are expected to maintain/back up their own critical files and data.

IV. COMPUTER SOFTWARE COPYRIGHT, SELECTION AND DUPLICATION:

It is the intent of the Tuscaloosa County School System to adhere to the provisions of copyright laws as they relate to computer/electronic software and/or applications. It is also the intent of the school system to comply with license agreements and policy statements contained in software packages used in the school system. The Board recognizes that computer software piracy is a major problem for the industry and that violations of computer copyright laws contribute to higher costs, necessitate greater efforts to prevent copying, and lessen incentives for the development of good educational software. All of these results are detrimental to effective uses of computers in the education setting. Therefore, in an effort to discourage violation of copyright laws and to prevent such illegal activities, the following guidelines shall control computer software selection and duplication in the school system:

A. The ethical and practical problems caused by software piracy will be taught to educators and students in all schools of the school system.
B. School system employees are expected to adhere to the provisions of the 1976 Copyright Act as amended in 1980 and the Digital Millennium Copyright Act of 1998 governing the use of computer software. Section 117 states that the owner of a computer program may make one copy of a program to be used as an archival copy unless licensing provisions obtained with the software state otherwise. Backup copies are not to be used on a second school computer at the same time an original is in use. A revision of the law passed in 1992 brought software piracy to felony status with fine up to $250,000 and up to five years in prison for systematic violations.
C. Software shall not be placed on a network system without a designated network version or a license agreement. When permission is obtained from the copyright holder to use software on a network system, efforts will be made to secure this software from illegal copying.
D. Illegal copies of copyrighted programs may not be created or used on school system equipment.
E. Any legal or insurance protection of the school system will not be extended to employees who intentionally violate copyright laws.
F. It is the responsibility of the Administrator at each work site to establish practices that will enforce the school system copyright policies.
G. All staff members (including instructional assistants) and students are expected to abide by the provisions of this policy.
H. Either the system Director of Technology of Technology or the local school Administrator is authorized to sign license acknowledgements for a school within the system. Copies of any system-wide license agreements must be signed by the system Director of Technology of Technology and/or Superintendent and distributed to all schools that will use the software. All binding contracts/agreements must be signed by the Superintendent.
I. The system technology staff is responsible for installation of all software in use on the wide area network. The system technology staff or the local Administrator or their designee is responsible for installation of all software in use on the local area network and/or individual devices within and purchased by Tuscaloosa County School System. Technology assistants or other designated staff may install software on technology devices with permission by the system Director of Technology of Technology and/or local school Administrator.

The following computer programs are permissible for use in classrooms throughout the school system:

1. Programs in the public domain (as long as the software applications do not provide utilities for hacking, bypassing, spying, or intentional disruption or non-approved access to the system's network resources.)
2. Programs covered by a licensing agreement with the software author, vendor, or developer, whichever is applicable.
3. Programs donated or loaned to the school (not illegal copies) having a written record that a bona fide contribution exists.
4. Programs purchased by individual schools and having a written record that a bona fide purchase exists.
5. Programs purchased by the user and having a written record that a bona fide purchase exists and can be produced by the user upon demand by the Superintendent or the Superintendent's designee.
6. Programs being reviewed or demonstrated by the user to reach a decision about possible future purchase or requested contribution or licensing.
7. Programs written or developed by school system employees and students for the specific purpose of use in the classrooms of the school system.
8. The Board, by this presentation, hereby notifies all employees and the general public of the intent of this policy.

It is also the policy of the school system that there is no copying of copyrighted or proprietary programs on computers belonging to the school system.

17 U.S.C. 106; Adapted with permission from policy statement approved by Board of Director of the International Council for Computers in Education. Definition: Copyright is a form of protection provided by the laws of the United States (title 17, *U. S. Code)* to the authors of "original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works.

V. EMAIL:

A. Tuscaloosa County School System provides access to email accounts for select student grade levels and all employees and long-term substitutes who require an email account and network access. The majority of employees including teachers are required to use the Exchange Outlook Webmail access. Administrators, clerical staff, and other employees who have static work areas are permitted to use the Outlook for their connectivity. Email accounts may be granted for school related organizations or classes with designated employee sponsors. (Note: The Outlook applications named herein are subject to change; therefore, in the event of a name or application change, this policy will remain in effect with the new applications as defined by the procedures from the Technology Department.)
B. Tuscaloosa County School System makes a reasonable effort to maintain/backup email for normal business operations. Backups are maintained as needed and controlled by the Technology Department. In addition, by federal law, the system is required to have in place a message archival system.
C. Technical support is provided for Tuscaloosa County School System email accounts used to conduct educational and/or instructional business.

D. Personal use of email is permitted as long as it does not violate Tuscaloosa County School System policy or adversely affect others or the speed of the network.
E. Use of Tuscaloosa County School System email accounts for harassing or threatening is strictly prohibited.
F. Tuscaloosa County School System email accounts may not be used for political activity, personal gain, commercial purposes, or profit. Unsolicited political or commercial email that is received from outside sources beyond our control is not considered a violation of this policy. However, local or state organizations that participate in political activity that contact our employees via system email may be blocked at the discretion of the board of education.
G. When using email, all users are responsible for maintaining professionalism at all times. Avoid impulsive and informal communication. Users must be constantly mindful of the need to review carefully and reconsider email communications before responding to and/or sending email. As a general rule, the content of an email should be acceptable to a general audience.
H. Tuscaloosa County School System email accounts may not be used for attempting to send or sending anonymous messages.
I. Tuscaloosa County School System email accounts may not be used for sending mass emails unless to parent lists or for other educational purposes.
J. Even though email is securely transmitted, discretion must be used when sending or encouraging the receipt of email containing sensitive information about students, families, school system employees, or any individuals. There can be no assurance that email will be confidential and/or private.
K. There is a system imposed limit on storage for email accounts. Users meeting or exceeding the limit will be unable to send or receive emails.
L. Users who require maintaining email(s) for more than 365 days should print said emails and file or store electronically in a different format.
M. Tuscaloosa County School System technology staff, administrative staff, and Tuscaloosa County Board of Education do not technically support or maintain individual user initiated email archives.
N. Incoming and outgoing email is filtered by the system for inappropriate content, viruses, phishing, and/or malware. However, no filtering system is foolproof, and material deemed inappropriate by individual users or harmful may be transmitted in spite of filtering. Tuscaloosa County School System cannot assume any liability for such breaches of the filter.
O. Email accounts will automatically expire on the last full day of employment.
P. At the discretion of the Director of Technology, email accounts may be locked without notice.

VI. INTERNET USE:

A. The intent of the Tuscaloosa County School System is to provide access to resources available via the Internet with the understanding that employees and students will access and use information that is appropriate for their various curricula or position.
B. All school rules and guidelines for appropriate technology usage as well as local, state, and federal laws apply to usage of the Internet.
C. Teachers should screen all Internet resources before projecting them in the classroom.
D. Students gain access to the Internet by agreeing to conduct themselves in a considerate and responsible manner and by providing written permission from their parents.

E. Students are allowed to conduct independent research on the Internet upon the receipt of the appropriate permission forms.
F. Permission is not transferable, and therefore may not be shared. Existing permission forms are valid until new forms are received. Students are required to have new forms signed each year or when changing schools.
G. Students who are allowed independent access to the Internet have the capability of accessing material that has not been screened and must follow all school rules and Technology Policy Guidelines as described within this policy.
H. Internet activity can and will be monitored along with other aspects of technology usage. Internet access for all users is filtered by the system through the content filters and policies. The Technology Department is responsible for monitoring all connections.
I. URLs (web addresses) and IP addresses may be added to or deleted from the filtered list by the Technology Department.
J. Users requesting sites for blocking or unblocking must list specific URLs.
K. Successful or unsuccessful attempts to bypass the Internet filter by using proxies or other resources are a violation of this policy.
L. Internet use refers to Internet access via all Tuscaloosa County School System private and public networks.

VII. WEB PUBLISHING:

A. The Tuscaloosa County School System web site is limited to usage associated with activities of Tuscaloosa County Schools. The web site cannot be used for profit, for commercial purposes, to express personal opinions, or to editorialize.
B. The Technology Department staff reserves the right to reject all or part of a proposed or posted web page.
C. All pages posted on the Tuscaloosa County School System web site must be designed/written with approved software applications or web portals.
D. It must be easy to determine the name or title of the person responsible for the content on each web page or sections of web pages housed on the Tuscaloosa County School System website.
E. A staff member's primary web page should be housed on the Tuscaloosa County School System web site.
F. Links from pages housed on the Tuscaloosa County School System website to personal blogs, social networking sites, advertisements unrelated to school system business, and/or personal web pages are prohibited.
G. Student pictures or other personally identifiable information such as name or grade level, etc., can be used in accordance with the signed "Tuscaloosa County School System Technology Usage Agreement" and in accordance with FERPA guidelines.
H. Student posting of personally identifying information of any kind on the Tuscaloosa County website or linking to personal information from the Tuscaloosa County School System website is prohibited. Personally identifying information includes home address, work address, home and/or cell phone numbers, social security number, etc.
I. Individual students may be identified by full name unless permission to do so is denied by the parent or guardian in writing on the *Technology Resource Agreement* form. Full names may

only be used in reporting student participation in school sponsored extracurricular activities, achievements, and other positive recognitions.

J. No written permission is required to list faculty/staff and their school contact information (phone extension, email address, etc.).
K. Permission for publishing employee photographs on the Tuscaloosa County School System website is assumed unless the employee specifies otherwise in writing to his or her direct supervisor.
L. Infringement of copyright laws, obscene, harassing, or threatening materials on websites are against the law and are subject to prosecution.

VIII. EXAMPLES OF INAPPROPRIATE 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 Management and Payroll data, accessed through school system technologies may not be used for any private business activity. The following are examples of inappropriate activities when using any Tuscaloosa County School System network, email system, hardware, software, technology services, and/or Internet access:

A. Using another user's password or attempting to discover another user's password.
B. Sharing passwords.
C. Trespassing in another user's files, folders, home Director of Technology, or work.
D. Saving information on any network drive or Director of Technology other than one’s personal home Director of Technology or a teacher-specified or approved location.
E. Downloading, installing, or copying software of any kind onto a computer, laptop, home Director of network drive, or other eDevice (except for approved updates or apps).

F. Harassing, insulting, embarrassing, or attacking others via technology resources including but not limited to using obscene, racist, profane, discriminatory, threatening, or inflammatory language in a document, email, blog, post, etc.
G. Damaging/abusing technology resources including but not limited to printers, telephones, computers, computer systems, any eDevice, or computer networks (includes changing workstation configurations such as screen savers, backgrounds, printers, BIOS information, preset passwords, etc.).
H. Intentionally wasting limited resources such as Internet bandwidth, disk space, and printing capacity.
I. Accessing inappropriate material stored on resources such as but not limited to digital cameras, flash drives, iPods, online storage, cell phones, websites, etc.
J. Accessing inappropriate material from websites or attempting to bypass the Internet filter to access websites that have been blocked (examples: information that is violent, illegal, satanic, sexual, demeaning, racist, inflammatory, and/or categorized as a social networking, blogging, or journaling site, etc.).
K. Sending, displaying, or downloading offensive messages or pictures.
L. Using a digital camera, camera phone, or any other device capable of storing a still or video image to take inappropriate, harassing, sexual, and/or embarrassing pictures.
M. Editing or modifying digital pictures with the intent to embarrass, harass, or bully is prohibited.

N. Participating in unsupervised or non-instructional on-line chat rooms without the permission/supervision of an adult staff member.
O. Posting any false or damaging information about other people, the school system, or other organizations.
P. Posting of any personal information as defined previously in this document.
Q. Broadcasting network messages or participating in sending/perpetuating chain letters.
R. Violating copyright laws.
S. Plagiarism of materials.
T. Use of technology resources to create illegal materials (i.e. counterfeit money, fake identification, etc.).
U. Use of any Tuscaloosa County School System technology resource is prohibited for personal gain or commercial or political campaign purposes with the exception of mentoring/tutoring services or fundraisers that benefit TCSS students or schools.
V. Accessing any website or other resources by falsifying information.
W. Downloading or playing games on-line that are not instructional in nature or without the permission of a teacher.
X. Streaming video or audio not related to the core instruction or business of the school system.

Email, Text Messaging, and Social Networking Guidelines

The purpose of these guidelines is to ensure the proper use of Tuscaloosa County School System email and Internet communication systems and to make users aware of what the Tuscaloosa County School System deems as acceptable and unacceptable use of its email and Internet communication systems and access to social network media while using system resources. We reserve the right to amend these guidelines as necessary. In case of revisions, users will be informed by email, by posts on the System Technology web page, through professional development, at faculty meetings, at grade level meetings, at department meetings, at assemblies, in class, and/or by other means deemed appropriate by the administration.

Email

Legal Risks

Email is a school business or educational communication tool, and users are obliged to use this tool in a responsible, effective, and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Any email is discoverable in a due process situation or other legal action. In addition, any email exchanged by a school system employee is public record. Other legal risks of email for Tuscaloosa County School System and/or their network users include the following:

- Sending emails with any libelous, defamatory, offensive, racist or obscene remarks;
- Forwarding emails with any libelous, defamatory, offensive, racist or obscene remarks;
- Forwarding confidential information;
- Forwarding or copying messages without permission or implied permission;
- Knowingly sending an attachment that contains a virus that severely affects another network.

By following the guidelines in this document, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in these guidelines, the user will be fully liable, and Tuscaloosa County School System will disassociate itself from the user as far as legally possible.

- Do not send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email containing libelous, defamatory, offensive, racist or obscene remarks, promptly notify your supervisor.
- Use caution if you forward a message without implied permission or without acquiring permission from the sender first, especially if it contains sensitive or personal information.
- Do not forge or attempt to forge email messages.
- Do not send email messages using another person's or a bogus email account.
- Do not copy a message or attachment belonging to another user without the permission or implied permission of the originator.
- Do not disguise or attempt to disguise your identity when sending email.

Best Practices

Tuscaloosa County School System considers email as an important means of communication and recognizes the importance of proper email content and of speedy replies in conveying a professional image and in delivering good customer service. The use of email in education, however, is proliferating, and the precise legal issues regarding appropriate use are yet to be determined. We are confident that—

- Any email exchanged by school system employees about individual students is public record.
- Any email pertaining to a particular student is discoverable in a due process situation or other legal action.
- The nature of email lends itself to impulsive, overly informal, and sometimes unprofessional communication.

Therefore, the Tuscaloosa County School System urges users to adhere to the following guidelines:

Guidance on Email between School Employees and Parents/Guardians

Examples of generally **appropriate** use of email between school employees and parents/guardians:

- Teachers invite parents to provide email addresses and then send out emails to those addresses reporting on classroom activities, projects, and assignments. These messages are generic and do not refer to specific students.
- Teachers may initiate or respond to email from a parent or guardian about a specific child, exchanging objective not subjective information such as the student's attendance, participation, homework, and performance in class.

Examples of **inappropriate** use of email between school employees and parents/guardians:

- Using email to report on serious problems regarding individual students.
- Using email to discuss confidential and sensitive matters, including:
- Medical/psychiatric/psychological diagnoses and treatments;
- Contents of special education and/or Section 504 evaluations, intervention plans, IEPs, 504 plans, disciplinary matters;
- Family problems and other sensitive family information.
- Using email language that is subjective, judgmental, unprofessional, pejorative, and/or labeling. Examples:
    - "Have you considered that Johnny might have ADHD?"
    - "Overall, I think that Johnny is unmotivated/lazy."

- "I don't think there is anything wrong with Johnny except his negative attitude."

Email between teachers and parents should be positive and/or general in nature when possible. Discussions involving serious problems and any and all protected information (medical, psychological, psychiatric, Special Education, Section 504, and disciplinary matters) should occur in person or by telephone.

Parents may initiate inappropriate email exchanges.

Example:

"Johnny is in your American history class and is failing. His father is an alcoholic and we are divorced. Johnny has ADHD and clinical depression. Can you please tell me how he is doing in your class and what I can do to help him?"

That kind of message should be deleted, and the teacher receiving it should call the parent who sent it. Alternately, the teacher could reply to it, deleting everything from the body of the email sent by the parent, and then respond with directions about how the teacher can be reached by telephone or in person.

Guidance on Email between School Employees Concerning Students

Examples of generally **appropriate** use of email between school employees:

- Emails that provide positive information, objective comments, and/or neutral information regarding school performance. In other words, conducting straightforward business, staying away from sensitive and confidential areas.

Examples of **inappropriate** use of email between school employees:

Using email to report on serious problems regarding individual students.

Using email to discuss confidential and sensitive matters, including:

- Medical/psychiatric/psychological diagnoses and treatments;
- Contents of special education and/or Section 504 evaluations, intervention plans, IEPs, 504 plans, disciplinary matters;
- Family problems and other sensitive family information.

Using email language that is subjective, judgmental, unprofessional, pejorative, and/or labeling.

Examples:

- "I think Johnny has ADHD."
- "Overall, I think that Johnny is unmotivated/lazy."
- "I don't think there is anything wrong with Johnny except his negative attitude."
- "I think this child's problem is his home life."

Discussions involving severe problems, subjective comments, and any and all protected information (medical, psychological, psychiatric, Special Education, Section 504, and disciplinary matters) should occur in person or by telephone.

General **Best Practices** involving all email are as follows:

Writing emails:

- Use short, descriptive **Subject:** lines.
- Avoid lengthy, detailed email messages. Consider using an attachment for "How To" information, directions, procedures, processes, or similar types of information.

- Avoid unnecessary attachments or large file attachments such as multiple pictures, mini movies, etc. AVOID USING ALL CAPITALS.
- If using cc or bcc feature, take steps to inform the cc or bcc recipient of any action expected unless the action is explicit in the email. The bcc option is often used to avoid revealing recipient email addresses to the entire group receiving the email; otherwise, the bcc option should be used sparingly if at all.
- If you forward emails, state clearly what action you expect the recipient to take.
- Use the spell checker before you send out an email.
- If the content of an email is not of a public nature,
- Consider using another form of communication or
- Protect the information by using a password.
- Only mark emails as important if they really are important.

Replying to emails:

- Emails should be answered within a timely manner, and at minimum employees are expected to check email at least once per work day during their contract term.
- Responses should not reveal confidential information and should be professional.

Newsgroups/ListServs:

Users should exercise caution before subscribing to a listserv, newsletter or news group. This type of email may be overwhelming, and cancelling a newsgroup and/or newsletter subscription is often difficult if not unsuccessful.

Maintenance

- Delete email messages in a timely manner (except for those that are part of a litigation hold situation).
- Print email messages required for documentation.
- Messages in the Deleted Items folder will be automatically removed in 3 days.
- A more frequent manual deletion of items by the individual user is recommended.
- User deleted emails will be permanently purged in 7 days.
- Messages in the Sent Items folder will be removed in 90 days. A more frequent manual deletion of items by the individual user is recommended.
- Emails older than 365 days will be removed from all email folders.
- Email accounts are assigned a mailbox size quota of 500MB. Failure to stay at or below the quota will result in the user being unable to send or receive email.
- Avoid responding to requests in emails that could be “phishing” attempts.
- Avoid opening attachments that are suspicious or mass forwarding virus hoaxes.
- Check with the technology staff when in doubt of the suspicious nature of emails.
- At the discretion of the Director of Technology, maintenance items listed above may be modified for special circumstances or users accounts.

Electronic Social Networking, Instant Messaging including Texting

Electronic social networking and/or instant messaging such as but not limited to Twitter, IM, or texting, among staff and students is a particularly sensitive matter in a time when growing numbers of school

employees maintain social networking accounts, email extensively in their personal lives, and are accustomed to using instant messaging services.

An absolute prohibition of communicating electronically with students seems excessive. On the other hand, teachers and school staff must maintain the highest standards should they choose to interact with students through electronic media. Below are some typical situations on which employees might need guidance.

Guidelines below are presented in a Q&A format.

Q: Is it ok for me to initiate electronic communications with a student?
A: If a teacher initiates overly personal contact with students outside of school, whether in person or electronically, he/she may create an impression of an unhealthy interest in students' personal lives and may leave himself/herself open to an accusation of inappropriate conduct; therefore, caution should be exercised in this type of communication.

Q: What if I receive an email or other electronic message such as a text from a student?
A: This very much depends on the nature of the communication received. Texting, instant messaging, or "chat"-type communication with students for purposes other than school related communications is strongly discouraged. If a communication is received that appears to be a social greeting, an employee might do best just to acknowledge it in an appropriate way at school. A very brief acknowledging electronic response might be appropriate in some circumstances. However, it is perfectly OK not to respond to such greetings. If an employee chooses not to respond, making an extra effort to greet the student cheerfully at school might be appropriate.

If a student sends a message with disturbing content, an employee should discuss this with his/her administrator or supervisor, including a school counselor in the discussion as needed.
If a student sends a message that appears to suggest an emergency, (an allegation of abuse or a student sharing suicidal thoughts or plans) try to contact an administrator or supervisor at once.

Q: *What about Facebook accounts or other social networking sites? Should I respond to an invitation to become a student's "Friend"?*
A: We recommend that employees not engage in online social networking with students unless the site is used for school information or academic reasons only. This would only be an issue, of course, if an employee chooses to maintain a Facebook or similar account. If an employee does so, we recommend that he/she be extremely cautious about the content of profiles and pages.
If an employee is strictly using a social networking site for school related topics and stays away from personal content, then these sites should be treated much like any other educational blog. However, the use of comments, "writing on walls," and so on would be likely to lead to major problems if an approval process is not in place before posting. Employees may find that it is easier to simply tell students that they have a policy not to accept students as "friends."

General Email Information
Virus Protection and Filtering

Incoming and outgoing emails sent to or received from the Tuscaloosa County School System exchange email server are scanned for viruses, spam, and content. However, users are expected to exercise caution when opening emails from unknown users or when using the web-based email client from home computers.

Incoming emails may be blocked if the message size is over 5MB or if there are multiple attachments that exceed this amount.

Disclaimer

Tuscaloosa County School System recommends that employees add a disclaimer to outgoing emails or automatically attach a disclaimer such as the one below to each email sent outside the school system. "This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to which they are addressed. If you have received this email in error please notify the system manager. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the Tuscaloosa County School System. Finally, the recipient should check this email and any attachments for the presence of viruses. The school system accepts no liability for any damage caused by any virus transmitted by this email."

System Monitoring

Users must have no expectation of privacy in anything they create, store, send, or receive on the Tuscaloosa County School System computer system. Emails can be monitored without prior notification if the Tuscaloosa County School System deems this necessary. If there is evidence that users are not adhering to the guidelines set out in this policy, the Tuscaloosa County School System reserves the right to take disciplinary action, including termination and/or legal action.

Email Accounts

Email accounts are assigned to new employees when their employment is approved by the Board of Education and when the new employee has read and signed acknowledgement and understanding of the Tuscaloosa County School System Technology Acceptable Usage Policy. All email accounts maintained on the Tuscaloosa County email and Internet communication systems are property of Tuscaloosa County School System. Tuscaloosa County School System maintains student accounts, employee accounts, and employee-sponsored accounts.

Passwords should not be given to other people and should be changed if the user believes his/her password is no longer secure. Email accounts are deleted immediately when employees retire, resign, or leave the school system for a period of six months or more. Only Tuscaloosa County School System employees are given email accounts. Upon request by the administration, Tuscaloosa County School System employee-sponsored accounts, such as PTA accounts, may be created. Employee-sponsored accounts are subject to these guidelines, and it is the responsibility of the sponsoring employee to educate the user of this and all other relevant technology-related policies and guidelines.

Electronic Communications and Internet access for Personal Use

Although Tuscaloosa County School System email and Internet communication systems are meant for school business, Tuscaloosa County School System allows the reasonable use of email and Internet for personal use if certain guidelines are adhered to:

- Personal use of email should not interfere with work.
- Personal emails must also adhere to the guidelines in this policy.
- Personal emails should be deleted regularly so as not to overburden the system.

The forwarding of chain letters, junk mail, inappropriate jokes, and executables is strictly forbidden.

Do not send personal mass mailings.

Do not send emails for personal gain, to solicit business for friends, family, etc., or for political purposes.

All messages distributed via the school system's email system including personal emails, are Tuscaloosa County School System property.

Internet use is permitted for personal use by employees as long as the use does not violate any of the rules or regulations of this policy and it does not interfere with the employee's work or job performance. Such permissible examples would include Internet shopping, travel or vacation research, news reports, etc. Please note this form of activity is however logged and could be requested by administration for review.

Questions
If you have any questions or comments about these guidelines, please contact your principal or immediate supervisor. If you do not have any questions, the Tuscaloosa County School System presumes that you understand and are aware of the rules and guidelines and will adhere to them.

Web Page and Web Publishing Guidelines
General Web Page Guidelines

Tuscaloosa County School System (TCSS) web pages are developed for curriculum and instructional use, school-authorized activities, or information about the Tuscaloosa County School System and its purpose.

- Text, graphics, audio, and/or video posted on any web-based page such as but not limited to web pages, wikis, on-line journals, blogs, Facebook, twitter sites, Moodle pages, Edmodo, glogs, voice threads, etc, qualify as "web pages."
- Web pages, pictures, and/or video/audio must adhere to *Tuscaloosa County School System Technology Usage Policy.*
- TCSS web pages cannot be used for profit or commercial or political purposes. All posted work must be of publishable quality with regard to spelling, usage, and mechanics. All web page authors are responsible for the maintenance of their own pages, including but not limited to adding new content, updating existing content, and deleting outdated content.
- All links should be checked regularly to make sure they are current and working. Pages that are not updated in a timely fashion, that contain inaccurate or inappropriate information, that violate copyright laws, or that contain links which do not work will be removed. The author will be notified.
- Unfinished pages should not be posted until they are fully functional.

- Staff and/or student work may be published only as it relates to a class project, course, or other school-related activity.
- Written permission is obtained from the student and guardian via the *Technology Resource Agreement* before posting student work on the Internet.
- No student's personal information, including but not limited to, phone numbers, email addresses, or mailing addresses may be posted on TCSS web pages.
- Staff is prohibited from linking to personal blogs, journals, and/or personal web pages from class or organization web pages.
- Employees should post and use school-sponsored email accounts for communicating with students and/or parents.
- Web pages are subject to approval by the System Director of Technology and local Administrator and must adhere to the regulations and restrictions established by the Tuscaloosa County School System.
- At minimum, each school's main page should include the school's name, address, phone number, fax number, and a link to Tuscaloosa County School System main page.
- Each web page should contain a link back to the previous level in the school's site and a link to the site's main navigational page.

- Pages that contain time-sensitive information, such as calendars, school events, staff information, etc., should be updated regularly.
- Unauthorized use of copyrighted material is prohibited.
- Links to sites that are not accessible inside the network (blocked by school filter) should not be used.
- The System Technology staff and/or local school Administrator may remove any web page(s) or content that is deemed inappropriate.
- "Guest books," "chat areas," "message boards," or similar tools must have curriculum value and should be evaluated by and approved by the System Director of Technology and local Administrator prior to use.

Technical Web Publishing Guidelines

- Pages should be sized so they will display properly in a variety of screen resolutions. Pages should be previewed and tested at least at "800 x 600" and "1024 x 768."
- Regular text entries on web pages should be limited to the standard fonts.
- Avoid color schemes or backgrounds that make the information on the page hard to read.
- Colors should be "web safe" as much as possible so that they will display.
- Photos should be sized and named appropriately. Photos should be in .jpeg format.
- Graphics should be used judiciously.
- The publisher may be asked to or the system or school's sub-site web editor may remove albums at any time if space or content becomes an issue.
- Animated GIF files should be used very sparingly and need to be relatively small. The amount, size, and type of graphics used have the most direct effect on the "load time" of web pages.
- Video and audio files may be used when they are appropriate and are compressed properly. They are generally large files that take long "load times" for the user and many times require

some users (non-system networked machines) to have special plug-ins or viewers/players in order to view or hear the files.

- Web pages should be easy to navigate and quick to load. Paths of information should be clearly defined while allowing for non-sequential browsing.
- Web pages should not be overcrowded.
- Full screen images and multiple images should be avoided whenever possible.
- Web page content and links should be checked and updated frequently.

Publishing Student Information

- Individual students may be identified by full name unless permission to do so is denied by the parent or guardian in writing on the *Technology Resource Agreement* form. Full names may be used in reporting student participation in school sponsored extracurricular activities, achievements, and other positive recognitions.
- Group photographs of students may be identified by the group name.
- Student photos or videos of students may be posted on the web with parent or guardian permission as indicated on the *Technology Resource Agreement*.
- No other personally identifying information about a student such as email address, phone number, home address, etc., is allowed.

Electronics Purchasing and Disposal Guidelines

This procedure is intended to provide for the proper purchasing and disposal of technology-related electronic equipment (including but not limited to computers, televisions, printers, monitors, fax machines, copiers, cell phones, data projector bulbs, copiers, etc.) hereafter referred to as electronic equipment. For further clarification of the term "technology-related electronic equipment," contact the Tuscaloosa County School System (TCSS) system Director of Technology.

Purchasing Guidelines

All electronic equipment that will be used in conjunction with Tuscaloosa County School System technology resources or purchased, regardless of funding, should be purchased from an approved list or be approved by the system Director of Technology. Failure to obtain approval of properly configured equipment prior to purchase may result in lack of technical support or denied access to technology resources.

All electronic equipment is subject to Alabama bid laws.

All electronic equipment over $250 should be inventoried in accordance with the Tuscaloosa County School System Finance Department guidelines using the approved Fixed Asset Form. It is the responsibility of the local school Administrator to inventory technology-related equipment used in the local school. The System Technology staff is responsible for ensuring that any network equipment, fileservers, and central office computers, printers, etc. are inventoried using the Fixed Asset Form.

Disposal Guidelines

Equipment should be considered for disposal for the following reasons:

- end of useful life;
- lack of continued need;

- obsolescence;
- wear, damage, or deterioration;
- excessive cost of maintenance or repair.

The local school Administrator, System Director of Technology, and the Director of Technology of Finance must approve school disposals by discard or donation. Written documentation including Fixed Asset number, description, and serial number must be provided to the System Technology Office using the appropriate form.

Methods of Disposal
Once equipment has been designated and approved for disposal, it should be handled according to one of the following methods. It is the responsibility of the local school Administrator to modify the appropriate Fixed Asset Form to reflect any in-school transfers, in-system transfers, donations, or discards. The System Technology staff is responsible for modifying the appropriate Fixed Asset Form to reflect any transfers within the central offices, transfers of central office electronic equipment to local schools, central office donations, or central office discards.

Transfer/Redistribution
If the equipment has not reached the end of its estimated life, an effort should be made to redistribute the equipment to locations where it can be of use, first within an individual school or office and then within the system. Service requests may be entered to have the equipment moved and reinstalled and, in the case of computer equipment, to have it re-ghosted and re-installed.

Discard
All electronic equipment in the Tuscaloosa County School System must be discarded in a manner consistent with applicable environmental regulations. Electronic equipment may contain hazardous materials such as mercury, lead, and hexavalent chromium.

A system-approved vendor must be contracted for the disposal of all electronic equipment. The vendor must provide written documentation verifying the method used for disposal and a certificate stating that no data of any kind can be retrieved from the hard drive or any other component capable of storing data.

Under no circumstances should any electronic equipment be placed in the trash. Doing so may make Tuscaloosa County School System and/or the employee who disposed of the equipment liable for violating environmental regulations or laws.

Donation
If the equipment is in good working order but no longer meets the requirements of the site where it is located and cannot be put into use in another part of a school or system, it may be donated upon the written request of the receiving public school system's superintendent or non-profit organization's Director of Technology.

It should be made clear to any school or organization receiving donated equipment that TCSS is not agreeing to and is not required to support or repair any donated equipment. It is donated AS IS.

Before offering donated equipment, TCSS staff should make every effort to ensure that the equipment is in good condition and can be re-used. Microsoft licenses are not transferable outside the Tuscaloosa County School System.

Donations are prohibited to individuals outside the school system or to current faculty, staff, or students of Tuscaloosa County School System. The donation of or sale of portable technology-related equipment is permissible to retiring employees if the following criteria have been met: a) the portable equipment has been used solely by the retiring employee for over two years; b) the equipment will not be used by the employee assuming the responsibilities of the retiring employee; and c) the equipment has reached or exceeded its estimated life. All donations and/or sales must be approved by the Finance Director of Technology and Director of Technology.

Required Documentation and Procedures

For purchases, transfers and redistributions, donations, and disposal of technology-related equipment, it is the responsibility of the appropriate technology team member to create/update the Fixed Asset Form to include previous location, new school and/or room location, and to check the appropriate boxes for transfer or disposal information. When discarding equipment, remove the fixed asset tag from the equipment and attach it to the fixed asset form. Copies of the forms should be sent to the local school bookkeeper or designated system level bookkeeper and a spreadsheet including all relevant information sent to the system technology office.

When equipment is donated, a copy of the letter requesting the equipment should be on file with the System Technology Office prior to the donation.

Any equipment that is being donated should be completely wiped of all data. This step will not only ensure that no confidential information is released but also will ensure that no software licensing violations will inadvertently occur. For non-sensitive machines, all hard drives should be fully wiped using a wiping program approved by the System Technology Office followed by a manual scan of the drive to verify that zeros were written.

Remove any re-usable hardware that is not essential to the function of the equipment that can be used as spare parts: special adapter cards, memory, hard drives, zip drives, CD drives, etc.

A system-approved vendor MUST handle all disposals that are not redistributions, transfers, or donations. Equipment should be stored in a central location prior to pick-up. Summary forms must be turned in to the System Technology Office and approved by the Finance Director of Technology prior to the scheduled pick up day. Mice, keyboards, and other small peripherals may be boxed together and should not be listed on summary forms.

Digital Devices During the Administration of a Secure Test

The possession of a digital device (including but not limited to cell phones, MP3 players, cameras, or other telecommunication devices capable of capturing or relaying information) is **strictly prohibited** during the

administration of a secure test. If a student is **observed in possession** of a digital device during the administration of a secure test, the device will be confiscated. If a student is **observed using** a digital device during the administration of a secure test, testing for the student will cease, the device will be confiscated and is subject to search, the student will be dismissed from testing, and the student's test will be invalidated. Additional disciplinary action may be taken by the school system.

Guidelines for the Search of Digital Device Seized During the Administration of a Secure Test:

- Assuming that a student is observed in the possession of or use of a digital device during the administration of a secure test, the device will be confiscated by the test administrator. "Smart phones" should temporarily be turned off to help prevent any remote-access data-wipe.
- The test administrator should deliver the device as soon as practicable to a school administrator.
- A "chain of custody" list should be kept to record everyone who had possession of the device and when the device was transferred to someone else. The device should be stored by the school administrator in a secure location until the next step is taken.
- For the purposes of determining whether a search of a digital device should take place, the school administrator should:
    - Learn the facts regarding the seizure of the device from the test administrator, and
    - Determine whether it is reasonable under all the circumstances to believe that the student could have been using the device to cheat or for some other un-permitted purpose.
- If the school administrator determines that the student was merely in possession of the digital device then it may be returned to the student in accordance with the Tuscaloosa County School System's procedure.
- If the school administrator believes that it is reasonable to suspect that the student was using the device for an impermissible purpose then he or she may search the device, limiting the search to only what is necessary to reasonably determine whether the student was cheating, copying secure test information, or violating a school rule.
- The school administrator should follow the local policy requirements regarding the search of student property.
- If no wrongful activity is discovered on the device then it may be returned to the student in accordance with the Tuscaloosa County School System's procedure.
- If wrongful activity is discovered on the device regarding the test at issue or, if other wrongful activity is inadvertently discovered on the device, then the school administrator should secure the device by storing it in a locked and secure location, and then notify the system test coordinator or Superintendent as appropriate.
- Following a search in which wrongful activity is discovered, and when the device is a "smart phone," the device should be turned off after the search to help prevent a potential remote-access data-wipe.
- Any disciplinary actions should be taken in accordance with the school system's disciplinary policy.
- Test irregularity reports should be completed in accordance with the Alabama State Department of Education's student assessment handbook.

REFERENCE(S): **CODE OF ALABAMA**
16-8-8, 16-13-231
CHILDREN'S INTERNET PROTECTION ACT (Public Law 106-554)

HISTORY: **ADOPTED: DECEMBER 9, 1996**
REVISED: MAY 10, 2004; JUNE 10, 2012; APRIL 8, 2013, JULY 16, 2015
FORMERLY: IFBGC, JFBGC