Coffee County School System Staff Acceptable Use Policy (AUP) rev.2013 approved 5/13/2013

The Coffee County School System (CCSS) provides students with access to computers, network systems, and other technology equipment so that teachers may use these tools as part of the instructional process. Teachers are responsible for providing educationally relevant lessons, supervision, and instruction to help students get the most benefit from available technology resources. All employees are responsible for using the systems in a manner consistent with the goals of the school system and to be respectful of other Users. This AUP and Internet Safety Policy adheres to the Children's Internet Protection Act (CIPA) [Pub. L. No. 106-554 and 47 USC 254(h)] and Tennessee Department of Education requirements as stated in Tennessee Code Annotated 49-1-221.

TECHNOLOGY RESOURCES

Technology equipment and other resources (i.e. email accounts) provided by the schools are the property of CCSS and are intended to be used by teachers, staff and students for educational purposes consistent with the goals of the school district. To maintain efficient functionality of the equipment and to ensure its appropriate use, the district reserves the right to monitor all network traffic, search all files and accounts stored on district-owned systems and to take such action as necessary to assure that system resources are available for their intended purposes. Therefore, employees should have no expectation of privacy when using school networks or technology equipment and resources. CCSS staff will protect the security and privacy of the network by not sharing passwords or other information with unauthorized personnel.

NETWORK SYSTEMS

School computer systems exist in a networked environment that is designed with safeguards to ensure its dependability but which also relies on the goodwill of its users. Employees who disrupt or compromise system resources by altering the network infrastructure or settings, attempting to acquire or use the login credentials of other users, introducing resource-draining applications, monitoring the network traffic of other users, bypassing existing security restrictions, or otherwise compromise the integrity of the network will be subject to disciplinary action and when applicable the involvement of appropriate law enforcement.

INTERNET ACCESS

The CCSS provides Internet and Email access to every school and should only be used for instructional and administrative purposes. In providing this access, the CCSS attempts to limit the availability of web content that is inappropriate for students in the school environment. While these restrictions are typically sufficient to protect the innocent, it is impossible to completely prevent students from accessing inappropriate material. Therefore, all employees are responsible for using the Internet and school email accounts in an appropriate manner and are permitted access only through the school's filtered Internet service. Employees are permitted to access the Internet and email only with a signed technology use agreement form. Employees who attempt to circumvent the filter system by either software or use of websites, access inappropriate Internet services or publish inappropriate content, or assist others in accessing or publishing such content or services may be subject to disciplinary action and when applicable the involvement of appropriate law enforcement.

Inappropriate uses of the CCSS network include, but are not limited to:

- Pornography
- Gambling
- Use of network for commercial purposes (Buying and selling for personal gain)
- Harassment, insulting, defaming or attacking others (Cyber Bullying)
- Violating Copyright Laws
- Illegal Activities
- Hacking or obtaining access to unauthorized systems
- Obscene Language
- Trespassing in other's files or folders
- Using another persons identity or password to access the network
- Damaging or modifying computer systems without permission from CCSS Tech Department

Even though CCSS blocks certain sites, the faculty and staff are expected to diligently monitor students' computer and Internet usage. CCSS runs filtering software as required by CIPA. The staff is always responsible for the supervision of students whenever they are using technology resources. The District Technology Department has the right to restrict the use/listening /watching of streaming media to preserve District bandwidth and the district will restrict the use of games for staff and students with the exception of educational software that has been approved by the CCSS Tech Department.

Coffee County School System Staff Acceptable Use Policy (AUP) rev.2013 (pg 2)

DOCUMENTS, FILES and SOFTWARE
The District technology staff has the right to remove any unauthorized or unlicensed software. Software should not be installed on any system without first getting approval from the District Technology Department to ensure compatibility with current systems and that there are no conflicts with any other systems. Staff should not alter copy, move or delete any files that belong to other staff members. Game, media or other files should not be downloaded and installed on any CCSS computer system without the permission of District Technology staff.

Student Personal Data – Staff should NEVER have student or staff records that contain date of birth and/or social security numbers on any device that leaves the CCSS property without proper security measures being in place. This data should never be entered into any online database or posted on any online or networked source unless approved by CCSS. Exceptions will be granted to CCSS personnel that have reason to do so. Permission must be given by the Director of Schools and security procedures vetted by the Director of Technology.

WEB SITES
CCSS has final editorial authority over websites that are stored on CCSS equipment or maintained in the Districts name. Student photographs or personal information should not be posted online without written permission from guardian.

STAFF COMPUTER, EMAIL AND DOCUMENT ACCOUNTS
Staff will be issued computer, email and document accounts. All staff accounts are accessible at any time by approved CCSS staff. Any abuse of the service (unprofessional activities, profanity and other violations stated by this AUP) may result in the staff's access of these services removed and are subject to disciplinary action and when applicable the involvement of appropriate law enforcement.

CHAT ROOMS, NEWSGROUPS, SOCIAL NETWORKS
Staff is not allowed to participate in chat rooms, newsgroups or social networks using the CCSS network unless it is provided by CCSS or has been given explicit permission.. Any circumvention or violation of this policy may result in disciplinary action and when applicable the involvement of appropriate law enforcement. Teachers may request access to these technologies, but the request must be made to the teacher's principal and then the principal request sent to the Director of Technology. It must be for educational purposes.

SCHOOL and PERSONAL DEVICES
Any staff member that checks out equipment (department laptops, etc) shall be responsible for it and are to make sure that the equipment is operating properly prior to it being checked out. It is the responsibility of the user to return the equipment in the same condition as when it was checked out (i.e. in proper working condition). Please refer to the Documents, Files and Software section of this document.

While personal computers, electronic devices and digital storage media can be beneficial to the educational process, such items also have the capacity to become distractions and to convey material that is unsuitable for the school environment. Therefore, employees may use personal computers, electronic devices and digital storage media only in a manner consistent with the goals of the school system. When brought onto school property, these devices are subject to search and may be confiscated pending review of appropriate disciplinary action. A staff person must gain permission from the tech director or his representative before any personal device can gain access to the CCSS network.

WARRANTY
Coffee County School District makes no warranties of any kind, whether expressed or implied, for the technology resources it provides. The district will not be responsible for damages suffered by students or staff in the use of technology resources including loss of data, interruption of services, and access to inappropriate content online.

INTERNET SAFETY

It is the policy of Coffee County School System to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)] and Tennessee Department of Education requirements.

Coffee County Schools recognizes the importance of keeping children safe online. To address this issue, the district will provide the following:

Internet Training to Students

Internet safety training to students in K-12 will be part of their regular instruction. Resources will be provided to classroom teachers and instruction time will be allotted. Education about safe and appropriate online behavior will be integrated into the K-12 curriculum and instruction. Students need to learn how to avoid inappropriate content and unwanted contacts from strangers while online as well as appropriate behavior on social-networking and chat-room web sites and the dangers of cyber bullying and to learn about protecting personal information.

Supervision and Monitoring

It shall be the responsibility of all members of the Coffee County School System staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act.

Evaluation and Review

The district will annually review its Internet safety program to make such adjustments as necessary. The Technology and Planning Committee will review and evaluate all aspects of the Internet Safety Policy and program annually and will recommend revisions as needed.

Professional Development Opportunities for Teachers and Staff in District

(1)Professional staff development will be provided in the following areas: Internet Safety in the Classroom, Curriculum Design, Internet Usage for Lesson Planning and Content, Usage of Digital Media and other appropriate technologies that will enhance or secure the learning environment of Coffee County Schools..

(2)Opportunities for faculty and staff to attend technology professional development workshops, conferences or other appropriate venues will be offered.

Our system will provide on-site, ongoing professional development for all faculty and staff, throughout the school year. This will be accomplished by scheduling in-service opportunities and after-school training to promote effective integration of technology in the classroom and library which will lead to student improvement and network security.

Assessment of the effectiveness of professional development will be measured by analyzing student achievement scores, classroom grades, teacher observations, and by sending periodic surveys to faculty and parents. A needs assessment will be conducted to sustain professional development activities that integrate technology effectively for the next school year.

Parental Involvement:

Student learning is maximized through familial or parental involvement in their schooling. However, family members may have very different levels of knowledge about instructional technology, and therefore varying capacity to become involved in a technology integrated learning process. Some parents do not understand the impact technology will have on their child's education as well as their child's post-high school employment prospects. In fact, many parents have a greater fear and misunderstanding of technology than do their daughters and sons. It is imperative to involve family members in the development of a school's technology plan and establish partnerships and include them in discussions and decisions. If parents are not involved, they may well oppose the plan based on fear rather than informed opinion.

The following are strategies that will be used in gaining parental involvement:

• Provide programs and/or speakers who can help parents, grandparents, caregivers, and community stakeholders understand how important it will be in the future for their children to be competent in safe technology use.

• Focus efforts to diminish parents' misconceptions, strengthen their technological awareness, and at the same time allow them to discover the potential of safe technology resources for their own uses.

• E-mail addresses of staff will be made available to parents and internet school sites will encourage communication between parents and teachers as well.

• Parents, grandparents, caregivers, and community stakeholders will be invited to attend the same meetings and training on safe technology usage that are held for the staff. As all participants are empowered with knowledge, they become more committed. As parents, grandparents, caregivers, and community stakeholders become better acquainted with teachers, they become more supportive.

Coffee County School System Staff Acceptable Use Policy (AUP)rev.2013

Acknowledgement Form

By signing below, I acknowledge that I have read and understand the Coffee County School System Staff Acceptable Use Policy and Internet Safety Policy and agree to follow this policy governing the use of Coffee County's network and computer systems. I understand that violation of the CCSS AUP policy could result in disciplinary/legal action in accordance with the AUP and the Coffee County Board of Education policies.

Name (printed)_____

Signature _____

Date _____

School or current assignment _____