ACCEPTABLE USE, INTERNET SAFETY and NETWORK SECURITY POLICY

The Choctaw County School District is pleased to make available to students access to a variety of technological resources and opportunities.

A. **GENERAL WARNING:** Individual Responsibility of Parents and Users. All users are advised that access to the network may include the potential for access to materials inappropriate for school-aged pupils. The legal and ethical practices and responsibilities of appropriate use of technology shall be communicated to all students and employees in the system. Every user must take responsibility for his/her use of the network and Internet and stay away from these sites. By signing this policy, users are taking full responsibility for his/her use and the District and all of the District's administrators, teachers, and staff shall not be responsible for any losses, damages or claims (including attorney's fees) of any kind, directly or indirectly, by any user or his/her parent or guardian.

If a student is under 18 years of age, he/she must have his/her parents or guardians read and sign the Policy. Users with a properly signed Agreement and who follows the Policy will have computer network and Internet access during the course of the school year. All users will be asked to sign a new Policy each year before they are granted access. Users, and if appropriate, the user's parents/guardians, may be asked to provide new or additional registration and account information, such information must be provided by the user (or his/her parent or guardian).
Note: A copy of all forms pertaining to this policy can be obtained by the school or by visiting the district website and navigating to the Technology Section.

B. Educational Purposes Only. All use of the network must be in support of education and research. If you have any doubt about whether a contemplated activity is educational, you should consult the person(s) designated by the District to assist you with such concerns.

C. Unacceptable Uses of the Network.
1. uses that violate the law or encourage others to violate the law; offer for sale or buy anything over the Internet; view, transmit, or download pornographic materials; download or transmit confidential, trade secret information.

2. uses that cause harm to others or damage to their property. For example, don't engage in defamation (harming another's reputation by lies, distribute, or redistribute jokes, stories, or other material which is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.); upload a harmful form of programming or vandalism; participate in any form of "hacking" unauthorized access to other computers, networks, or information systems. All users must abide by rules of network etiquette such as using appropriate language.

3. do not disclose private information about you or others which might allow a person to locate you without permission. (ex. credit card numbers, social security numbers, and your name or address) Do not arrange a face-to-face meeting with someone you "meet" on the Internet.

4. other specific content and actions that are prohibited include, but not limited to, the following:
- Political lobbying.
- District and school budget figures.
- Engaging in network packet sniffing or snooping.
- Operating network servers of any sort in violation of guidelines.
- Setting up a system to appear like another authorized system on the network (Trojan)
- Attempting to by pass security for information resources
- Assisting someone else or requesting someone else to bypass security

I. WORLD WIDE WEB (Websites) - The official system/school website shall be governed by all provisions of this policy. Authorized personnel designated to update system/school web pages will make sure that the following standards are observed:

- Only "official pages" - those whose content has been subject to strict adult editorial control, complying with standards set by the CCBOE and the School and containing no offensive material, nor any third party copyright item, unless permission has been obtained - are allowed to become part of the system/school website. (See Copyright Web Publishing Rules and Copyright Permission Letter on district website)
- Before publishing student work on the website, an authorization form must be obtained from the parent or guardian. No student names may appear without a signed Internet Publishing Permission, adhering to guidelines as indicated on the form.
- Any links to websites outside the school's or school district's pages must comply with the CCBOE policy on Internet usage and the curriculum.
- Teachers who wish to create and maintain individual class pages may do so. These class pages must comply with this policy on creation and maintenance of system/school web pages.

II. EMAIL - The Board provides access to email for employees. Access is intended to support educational, instructional, or normal administrative activity. Board policies and procedures shall apply to the use of email. Privacy or security of any information cannot be guaranteed.

III. COPYRIGHT WEB PUBLISHING RULES

1) Unauthorized use, storage or distribution of copyrighted materials is a policy violation.
2) Copyright law and district policy do not allow the re-publishing of text or graphics found on the Web or district websites or file servers without explicit written permission. For each republishing (on a web site or file server) of a graphic or a text file which was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. In many cases, that notice should also include the URL (web address) of the original source.
3) Before the web pages containing text and/or graphics from other sites are actually published, students and staff engaged in producing those pages must obtain permission from the copyright holder of the materials to re-publish those materials on the system/school site. Such permission must be either a letter or printed e-mail from the copyright holder, which will be held on file. In the case of "public domain" documents and printed evidence must be provided to document the status of the materials.
4) The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text. Student work may only be published with written permission from the user or, if the user is a minor, the user's parent or guardian.

IV. NETWORK SECURITY - Physical access to networking equipment (routers, switches, hubs, etc.) is not permitted without the prior approval of the IT Department. The IT Department will provide a general method for network authentication. Any use of the network must be in conformity to state and federal laws, licenses, and District policies. The user or, if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with the District in the event of an investigation.

The District reserves the right to identify the appropriate network security level for systems and users. System accounts are to be used only by authorized users for the authorized purpose. Users may not share passwords or leave an open file or session unattended. Account owners are ultimately responsible for all activity under their accounts. Users will be required to change passwords regularly. Users shall not obtain copies of, modify files, data, or passwords belonging to other users, misrepresent other users on the network, or attempt to gain unauthorized access to the network. Network components, including hardware or software shall not be destroyed, modified or abused in any way. Any device found to be causing problems to the network or in violation of this policy, is subject to disconnection.

V. STUDENT-OWNED DEVICES - Bring Your Own Technology for Educational Purposes
In an effort to meet the needs of today's 21st Century students and staff, the District is allowing students and staff to bring personal digital devices on campus for educational purposes. All staff is encouraged to utilize the advantages of student-owned devices in their classroom for learning. Users must adhere to Student Code of Conduct and all Board Policies. Responsibility to keep the device secure rests with the individual owner. It is recommended that custom details are used to physically identify devices.

Allowable devices are: Internet enabled phones (iPhones, Android, Blackberry, etc.), eReaders or types of electronic textbooks with Internet capabilities (Nook, Kindle, etc.), Laptops, Netbooks, Tablets, any other devices must be approved by the IT Department. Virus protection is recommended.

Additionally personal digital devices:

- Must be in silent mode while on campus and while riding buses
- Must be charged and "ready to use", not used until directed/need in class. Games are not permitted.
- Will not be used during test or state assessments (see district policy for digital devices during testing).
- May not receive maintenance (troubleshooting or repair) by district staff.
- Are permitted to access personal data plan providers. Users are expected to adhere to all Board policies.
- Will not be used to post to social networks during the school day unless authorized by a teacher or administrator for educational purposes
- Files may have to be saved on your personal device, jump drive, external drive or alternate media/device.
- Printing from digital devices will not be possible at school unless specifically authorized.

VI. PRIVACY - For security purposes, the District reserves the right for authorized personnel to monitor, copy, review, and store without prior notice any usage of the district network. Reasonable cause may be provided by a complaint of a policy violation or as incidentally noticed while carrying out normal duties of the IT Department. The District will utilize filtering software or other technologies to prevent students from accessing visual depictions that are obscene or harmful to minors. Internet filtering software or other technology-based protection systems may be disabled as necessary.

VII. FAILURE TO FOLLOW POLICY - A user violates this Policy by his/her own actions or by failing to report any violations by other users.

The District may take the following Disciplinary Actions:

1. Sending a Warning to parent and student about Policy guidelines
2. Loss of privileges for one Week
3. Loss of privileges for one Month
4. Permanent loss of privileges
5. Disciplinary actions as outlined in the District Cell Phone/Digital Device in a Testing Setting
6. Other disciplinary actions as set by Superintendent and Board of Education

Note: A copy of all forms pertaining to this policy can be obtained by contacting a school or by visiting the System website and navigating to the Technology Section.

REFERENCES: **CODE OF ALABAMA**
16-8-8, 16-12-3, 16-13-231

HISTORY: **ADOPTED: SEPTEMBER 25, 2001**
REVISION DATE(S): APRIL 5, 2011, APRIL 12, 2016
FORMERLY: JT