

CHAPTER 5.00 - STUDENTS

should be reported to the Director of Technology. Teachers may also request that sites be opened for periods of research.

The Internet: The intent of the Chickasaw City School System is to provide access to resources available via the Internet with the understanding that faculty, staff, and students will access and use only information that is appropriate, beneficial, and/or required for his/her various curricular or extracurricular activities or staff duties.

- Internet access is provided to allow students, faculty, and staff to conduct research. Users will gain access to the Internet by agreeing to conduct themselves in a considerate and responsible manner. Students must provide written permission from legal custodial parents, a signed copy of permission to use Internet resources for each student in the household. Students will not be allowed to conduct independent research on the Internet until receipt of the signed form.
- The board provides technology protection measures that include blocking or filtering Internet access to visual depictions and text that are obscene, pornographic, or harmful to minors. These measures cannot be considered 100% effective. Teachers will screen resources that will be used in the classroom for content prior to their introduction, and shall observe students using the Internet. Sites that are deemed inappropriate or a disruption of the learning atmosphere are to be reported to the Technology Coordinator. Teachers may also request specific sites to be opened for the purposes of research.
- Network users are prohibited from accessing external networks or alternate Internet service providers within Chickasaw City school's internal network unless expressly authorized by the Superintendent or Superintendent's designee and properly protected by a firewall, other appropriate security device(s), and appropriate filtering software.
- All school rules and guidelines for appropriate technology use shall apply to use of the Internet. Because communications on the Internet are often public in nature, all users must engage in appropriate and responsible communications with particular regard to avoiding disruption of the educational environment.
- Student posting of personal information of any kind about themselves or others is prohibited. Personal information includes home and/or school addresses, work addresses, home and/or school phone numbers, names, social security numbers, pictures, etc. The board cannot guarantee the privacy, security, or confidentiality of any information sent or received via the Internet.

System, school, and school-sponsored activity web sites: Because any school system web sites can be globally available and represent the community at large, the designated school system webmaster will review all web sites and/or new features and links before adding them to the system's web site. Only the designated school system webmaster may place web sites, features, or links on the web server. The webmaster may reject all or part of proposed home pages and/or new features and links for any reasons. The legal and ethical practices and responsibilities of appropriate use of technology resources shall be taught to all students and employees in the system (i.e. during lab orientation, network orientation, faculty meetings, etc.).

CHAPTER 5.00 - STUDENTS

Student-Owned Devices (BYOD): In an effort to expand students' 21st century learning opportunities, Chickasaw City Schools has implemented an initiative that allows students to bring their own digital devices on campus for educational purposes. It is imperative that these devices be used appropriately. Rules governing the use of student-owned digital devices in our schools include the following:

Devices Allowed: Student-owned devices, unless expressly prohibited by the principal and/or Technology Coordinator, shall be allowed.

Student Responsibilities: Students will abide by all school/system rules and policies, including this policy and Code of Student Conduct. Use of the device will only be allowed when permissible according to a school administrator or designee. Students are not permitted to transmit or post any photographic images or videos of any person on campus on any public and/or social networking sites without prior approval from a school official.

Students will only be allowed access to websites and resources which are relevant to the curriculum and content in the classroom. Students must understand that infecting the network with any virus designed to damage, alter, destroy or limit the network's effectiveness is a violation of the Acceptable Use Agreement and this policy, which will result in disciplinary actions. The school/system has the right to confiscate and examine any device that is suspected of causing problems or is the source of an attack or virus infection.

Network Access: Students will only use the school's wireless guest network. This network is controlled by the system's technology department and is filtered according to Children's Internet Protection Act (CIPA) guidelines. At no time will the guest network settings be altered for device specific needs. The school system's guest network, while reliable and stable, will, at times, experience outages. No guarantee will be made that it will always be available.

Additionally, signal strength could vary depending on the number of devices connected and the proximity to an access point. There will be no expectation of access to electrical outlets for charging purposes. Students must bring devices that are fully charged to school. The Chickasaw City School System will not be responsible for any loss of data resulting from connecting to the network. The Chickasaw City School System does not provide troubleshooting assistance or repair for student owned devices. Teachers are not responsible for student connectivity or for helping students who experience trouble connecting to the guest network.

Theft/Damage of Devices: The schools/system will not be responsible for lost or stolen devices. Physical damage or loss of data is not the responsibility of the school or the school system. As with any items on school campuses, school officials may inspect any personal device when there is reasonable suspicion that contents are a violation of policies, or of any local, state, or federal laws.

Violations: Individuals are expected to report any violations of this policy and/or problems with the security of any technology resources to the principal and/or Technology Coordinator.

All school system technology resources, regardless of purchase date, location, or fund sources (including donations), are subject to this policy.

Students who misuse the school system's technology will be subject to consequences as specified in the Code of Student Conduct. Employees who misuse the school system's technology may be subject to

CHAPTER 5.00 - STUDENTS

appropriate consequences, up to and including possible termination. Violation of civil and/or criminal law relating to technology and its use will result in the notification of law enforcement officials.

References: Code of Alabama 16-11-9, Child Internet Protection Act

5.91 INFORMATION MANAGEMENT SYSTEM AND STUDENT DATA

The Chickasaw City School System shall develop and maintain an integrated information system for educational data management. The Superintendent or designee shall ensure compatibility exists with the state information systems. Procedures and guidelines shall be developed to ensure that adequate management information support needs are met. In addition, the Superintendent is authorized by the board to develop plans and procedures to maintain data security.

The Chickasaw City School System adheres to all aspects of the Family Educational Rights and Privacy Act (FERPA) as it implements programs and procedures for collecting, managing, storing, transmitting, using, securing, reporting, and destroying data and student information. Appropriate use of data is essential to student achievement, planning, and school system program effectiveness.

School system data collection, management, and reporting is implemented according to Alabama State Department of Education guidelines and in a manner designed to preserve and protect individual and collective privacy rights and to ensure confidentiality and security of collected data. Local school and system student data is transmitted daily to the Alabama State Department of Education data management system from which state and federal reporting is completed. Each student is assigned a unique student identifier upon enrollment into the student management system to ensure compliance with the privacy rights of each student and his or her parents/guardians. No personally-identifiable individual student data is shared in either state or federally-required reporting.

Data collected by the school system is maintained within a secure infrastructure. Access to data is limited to staff whose job responsibilities include required data collection, analysis, reporting, and management. Training in data security and student privacy laws is provided to these individuals on a regular basis to ensure compliance with school system policies and state and federal privacy laws.

References: Code of Alabama 16-11-9, Family Educational Rights and Privacy Act of 1974; Alabama State Board of Education Data Use and Governance Policy (Oct 10, 2013)