

4.8.13 Access to Internet and Technology Resources.

The ~~intent of the~~ Board ~~permits is to provide~~ restricted and conditional access to and use of its technology resources, including but not limited to computers, ~~available via~~ the Internet, network storage areas and electronic mail, to employees, students and other persons who are engaged in bona fide educational and administrative activities that serve, and are consistent with identified educational objectives or authorized support functions, and who agree to abide by all Board policies, rules, and regulations regarding technology use. Access to the Internet is provided with the explicit understanding that faculty, staff, and students will access and use only information that is appropriate, beneficial, and/or required for various curricular or extracurricular activities or staff duties. Teachers will screen resources that will be used in the classroom for instructional content prior to their introduction. Board policies and procedures shall apply to use of the Internet.

- a. Internet access is provided to allow students, faculty and staff to conduct research and access resources. Users gaining access to the Internet agree to conduct themselves in a considerate and responsible manner. By signing the Code of Student Conduct and the Student/Parent Device Agreement Form for each student in the household, legal custodians/parents provide written permission for their child to have access to the Internet and network resources.
- b. 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 and has authorized the Superintendent to develop additional or more specific rules consistent with the provisions in sub-section (g) below. These measures cannot be considered 100% effective. Teachers must preview websites being used for instructional purposes and observe students using the Internet. Teachers are responsible for monitoring and overseeing student use of computers and online resources in accordance with this Acceptable Use Policy, and for educating students about digital safety and ethics as well as integrating into their teaching the Technology Course of Study. If a student encounters inappropriate content online, they are to immediately close the browser and report the incident to the teacher. Sites that are deemed inappropriate or a disruption of the learning atmosphere should be reported to the DoT. Teachers may request blocked sites be opened which they feel are appropriate and needed for instruction by contacting the Technology Department.
- c. Sites found to disrupt the learning atmosphere by consuming excessive internet bandwidth may be blocked or otherwise limited at any time without notice.
- d. Network users are prohibited from accessing external networks or alternate Internet service providers while within the Madison City Schools' 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. This prohibition

includes, but is not limited to, VPN or other technologies that attempt to bypass district filters/security, cellular “hot spots”, cellular data plans, etc.

e. 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.

f. Employees and students should be aware that posting of personal information of any kind about themselves or others is prohibited. Personal information includes home addresses, work addresses, home phone numbers, social security numbers, etc.

g. The Superintendent is authorized to develop additional or more specific rules and regulations regarding access to and use of its technology resources and to require adherence to such rules and regulations through the “Acceptable Use Policy,” amendments to Board policies, or to the Student Code of Conduct, and application of appropriate disciplinary policies and procedures. Those rules and regulations should incorporate the requirements of the federal Child Internet Protection Act and Alabama’s Freeing our Classrooms of Unnecessary Screen for Safety (“FOCUS”) Act by:

Blocking or filtering internet access to pictures that are obscene, that constitute child pornography, or that are harmful to minors;

Restricting access by minors to inappropriate and harmful material on the Internet;

Limiting Internet access by students to only age-appropriate subject matters and materials;

Providing specific procedures and other protections that prioritize the safety and security of students when using email, chat rooms, and other forms of direct electronic communication;

Preventing “hacking” and other forms of unauthorized use of or access to computer or Internet files, sites, databases, or equipment;

Prohibiting access by student to unlawfully obtained data or information, including “hacking” and other unlawful online activity by students;

Prohibiting access to websites, web applications, or software that exposes students to the disclosure, use, or dissemination of their personal information;

Prohibiting students from accessing social media platforms, unless expressly directed by a teacher for educational purposes;

Unauthorized disclosure, use, and dissemination of personal information regarding minors;

Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.