Policy 4.29

INTERNET SAFETY AND ELECTRONIC DEVICE USE POLICY Effective: 5/19/2015

Definition

For the purposes of this policy, "electronic device" means anything that can be used to transmit or capture images, sound, or data.

The District makes electronic device(s) and/or electronic device Internet access available to students, to permit students to perform research and to allow students to learn how to use electronic device technology. Use of district electronic devices is for educational and/or instructional purposes only. Student use of electronic device(s) shall only be as directed or assigned by staff or teachers; students are advised that they enjoy no expectation of privacy in any aspect of their electronic device use, including email, and that monitoring of student electronic device use is continuous.

No student will be granted Internet access until and unless an Internet and electronic device use agreement, signed by both the student and the parent or legal guardian (if the student is under the age of eighteen [18]) is on file. The current version of the Internet and electronic device use agreement is incorporated by reference into board policy and is considered part of the student handbook.

Technology Protection Measures

The District is dedicated to protecting students from materials on the Internet or world wide web that are inappropriate, obscene, or otherwise harmful to minors[1]; therefore, it is the policy of the District to protect each electronic device with Internet filtering software[2] that is designed to prevent students from accessing such materials. For purposes of this policy, “harmful to minors” means any picture, image, graphic image file, or other visual depiction that:

A. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
B. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
C. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Wireless Networks Measures

A. RSD shall ensure all wireless access shall require authentication and utilize WPA2 (256 bit keys), or better, encryption methods for data transport.

B. RSD wireless networks will be separate for guests, students and staff/faculty, utilizing VLANs and Access Control Lists to keep this separation.

C. RSD shall ensure that wireless networks will deploy network authentication and encryption in compliance with the Arkansas State Security Office's Best Practices.

D. RSD shall scan for, and disable, rogue wireless devices at a minimum monthly. Scans will be made utilizing 3rd party vendor wireless controller's heat maps and walkthroughs with end-users devices.

Internet Use and Safety

The District is dedicated to ensuring that students are capable of using the Internet in a safe and responsible manner. The District uses technology protection measures to aid in student safety and shall also educate students on appropriate online behavior and Internet use[3] including, but not limited to:

A. interacting with other individuals on social networking websites and in chat rooms;
B. Cyberbullying awareness; and
C. Cyberbullying response.

Misuse of Internet

The opportunity to use the District's technology to access the Internet is a privilege and not a right. Students who misuse electronic devices or Internet access in any way will face disciplinary action, as specified in the student handbook[4] and/or Internet safety and electronic device use agreement. Misuse of the Internet includes:

A. The disabling or bypassing of security procedures, compromising, attempting to compromise, or defeating the district's technology network security or Internet filtering software;
B. The altering of data without authorization;
C. Disclosing, using, or disseminating passwords, whether the passwords are the student's own or those of another student/faculty/community member, to other students;
D. Divulging personally identifying information about himself/herself or anyone else either on the Internet or in an email unless it is a necessary and integral part of

the student's academic endeavor. Personally identifying information includes full names, addresses, and phone numbers.

E. Using electronic devices for any illegal activity, including electronic device hacking and copyright or intellectual property law violations;
F. Using electronic devices to access or create sexually explicit or pornographic text or graphics;
G. Using electronic devices to violate any other policy or is contrary to the Internet safety and electronic device use agreement.

Legal Reference: Children's Internet Protection Act of 2001, PL 106-554, FCC Final Rules 11-125 August 11, 2011, 20 USC 67777, 47 USC 254(h)(l), 47 CFR 54.520, 47 CFR 5209(c)(4), A.C.A. § 6-21-107, A.C.A. § 6-21-111
Adopted: 2/20/2012
History BOE: 2/20/2012, 5/11/2015
Revised: 5/19/2015