Colorado Springs School District 11
Board of Education Policy
JS, Technology Resources and Internet Safety
Responsible Use for Students
Revised May 29, 2019

TECHNOLOGY RESOURCES AND INTERNET SAFETY RESPONSIBLE USE FOR STUDENTS

Technology and electronic resources provide access to a wealth of information and services to students and staff. Colorado Springs School District 11 (the “District”) believes technology should be used in schools as a learning resource to educate and inform. The District supports the use of the Internet and electronic communications by staff to improve teaching and learning through interpersonal communication, access to information, research, training and collaboration and dissemination of successful educational practices, methods and materials. For purposes of this policy, "District technology device" means any District-owned computer, hardware, software, or other technology that is used for instructional or learning purposes and has access to the Internet. Use of the Internet and electronic communications requires students to think critically, analyze information, write clearly, use problem-solving skills and hone computer and research skills that employers demand. Use of these tools also encourage an attitude of lifelong learning and offers an opportunity for students to participate in distance learning activities, ask questions of and consult with experts, communicate with other students and individuals and locate material to meet educational and personal information needs.

BLOCKING OR FILTERING OBSCENE, PORNOGRAPHIC AND HARMFUL INFORMATION

To protect students from material and information that is obscene, child pornography or material or information otherwise harmful to minors, technology that blocks or filters such material and information shall be installed on all District computers having Internet or electronic communications access prior to issuing to students. Students shall report access to material and information that is inappropriate, offensive or otherwise in violation of this policy to the supervising staff member. If a student becomes aware of other students accessing such material or information, he or she shall report it to the supervising staff member.

The District reviews and evaluates electronic resources throughout the school year that comply with Board policies that govern the selection of instructional materials. Students may be able to navigate beyond instructional resources that have been evaluated prior to use.

STUDENT USE IS A PRIVILEGE

Use of the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Student use of the Internet, electronic communications and District technology devices is a privilege, not a right. Students will practice digital responsibility when using devices and electronic systems including Internet and email. Open attachments only from trustworthy sources, and be mindful of spams or scams. Chain emails shall not be forwarded to District users. Failure to follow the use procedures contained in this policy shall result in the loss of the privilege to use these tools and restitution for costs associated with damages, and may result in disciplinary action and/or legal and/or disciplinary action including suspension and/or expulsion, in accordance with Board policy concerning suspension, expulsion and other disciplinary interventions. The District may deny, revoke or suspend access to District technology or close accounts at any time.

AUTOMATIC ACCESS

Student access to the internet in the District as an educational resource is automatic unless a parent or guardian notifies the school in writing that they are opting their student out of automatic Internet access, as required by Board Policy IMBB, Exemptions from Required Instruction. (see Board Policy IMBB and Exhibit JS-E-3).

NO EXPECTATION OF PRIVACY

District technology devices are owned by the District and are intended for educational purposes at all times. Students shall have no expectation of privacy when using District technology devices and technology systems such as productivity tools, email and file storage. The District reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of District technology devices, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through District technology devices shall remain the property of the District.

UNAUTHORIZED AND UNACCEPTABLE USES

Students shall use District technology devices and electronic resources in a responsible, efficient, ethical and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of District technology devices and electronic resources cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following:

No student shall access, create, transmit, retransmit or forward material or information:

- that promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons
- that is not related to District education objectives
- that contains pornographic, obscene or other sexually oriented materials, either as pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion
- that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the District's nondiscrimination policies
- for personal profit, financial gain, advertising, commercial transaction or political purposes
- that plagiarizes the work of another
- that uses inappropriate or profane language likely to be offensive to others in the school community
- that is knowingly false or could be construed as intending to purposely damage another person's reputation
- in violation of any federal or state law or District policy, including but not limited to copyrighted material and material protected by trade secret
- that contains personal information about themselves or others, including information protected by confidentiality laws
- using another individual's Internet or electronic communications account without written permission from that individual
- that impersonates another or transmits through an anonymous remailer

- that accesses fee services without specific permission from the District-level system administrator

Security on District technology devices is a high priority. Students who identify a security problem while using District technology devices must immediately notify a system administrator. Students should not demonstrate the problem to other users. Logging on to the Internet or electronic communications as a system administrator is prohibited.

Students shall not:

- use another person's password or any other identifier
- gain or attempt to gain unauthorized access to District technology devices
- read, alter, delete or copy, or attempt to do so, electronic communications of other system users

Any user identified as a security risk, or as having a history of problems with technology, may be denied access to the Internet, electronic communications and/or District technology devices.

PERSONAL DEVICES

Personal devices are allowed, and their educational use is encouraged. Students who elect to use their own device must conform to this and other District policies while the device is using District network/Internet resources. Students are responsible for keeping device updated, daily operation and safety of their device.

SCHOOL DISTRICT MAKES NO WARRANTIES

The District makes no warranties of any kind, whether expressed or implied, related to the use of District technology devices, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by the District of the content, nor does the District make any guarantee as to the accuracy, age appropriateness, or quality of information received. The District shall not be responsible for any damages, losses or costs a student suffers in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the student’s own risk.

It is possible to access material that students (or parents/guardians of students) might find inappropriate. While the District will take reasonable steps to restrict access by minors to harmful material including the use of an Internet content filter, it is impossible to guarantee that such access cannot or will not be gained.

SAFETY

Students shall not reveal personal information or personal information of other individuals, such as home address or phone number, while using the Internet or electronic communications. Without first obtaining permission of the supervising staff member, students shall not use their last name or any other information that might allow another person to locate him or her. Students shall not arrange face-to-face meetings with persons met on the Internet or through electronic communications.

VANDALISM

Vandalism will result in cancellation of privileges and may result in school disciplinary action and/or legal action. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse or disrupt the operation of any network within the District or any network connected to the Internet. Vandalism is also defined as any malicious or intentional attempt to harm the operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or District technology device. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

ASSIGNING STUDENT PROJECTS AND MONITORING STUDENT USE

The District will make reasonable efforts to see that the Internet and electronic communications are used responsibly by students. Administrators, teachers and staff have a professional responsibility to work together to monitor students' use of the Internet and electronic communications, help students develop the intellectual skills needed to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet their educational goals. Students shall have specifically defined objectives and search strategies prior to accessing material and information on the Internet and through electronic communications.

UNAUTHORIZED CONTENT – SOFTWARE AND APPLICATION PROCESS

The District requires that all software applications used on District devices be submitted for testing and approval to appropriate personnel before installation. Students are prohibited from using or possessing any software applications, mobile apps or other content that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any applicable fees.

USE OF SOCIAL MEDIA

The District realizes the changing methods of communication and teaching include social media. Social networking websites have the potential to support student learning, and staff and students can participate in online social networks where people all over the world share ideas, collaborate, engage community and create new learning. The District schools and programs may have a presence in social networking sites. As such, the District seeks to provide both a safe, secure learning environment and the opportunity for students to learn. The District adopts the approach of helping students become responsible users of digital media and personal responsibility is expected. Teacher/Student interactions online must only occur within the context of educational usage. For the protection of both students and staff, the District strongly advises that staff do not “friend” students in public social media sites, since the lines of personal and professional boundaries are not as clear in the social networking sites. “Friending” or “Following” students on private or school-based networks for educational purposes is acceptable within the context of educational usage (i.e. Library software, Learning Management Systems, etc.)

Adopted March 1996
Revised June 1999
Revised September 2001
Revised February 2003

Revised March 16, 2011
Revised June 19, 2013
Revised April 27, 2016
Revised May 29, 2019

CROSS REFS.:

AC, Equal Opportunity
EGAD, Copyright Compliance
GBAA, Employee Sexual and Racial Harassment/Discrimination
GBEE, Technology Resources and Internet Safety Responsible Use for Staff
GBEE-E-1, Appropriate Use of Technology Resources and Internet Safety Responsible Use by Staff
GBEE-E-2, Staff Electronic Device Letter of Agreement
IMBB, Exemptions from Required Instruction
JBB Sexual and Racial Harassment/Discrimination towards Students
JIC, Student Code of Conduct
JICDE, Bullying Prevention and Education
JK and JK-R, Student Discipline
JRA/JRC Student Records/Release of Information on Students
Student Conduct and Discipline Code
JS-E-1, Appropriate Use of Technology Resources and Internet Safety Responsible Use by Students
JS-E-2, Student Electronic Device Letter of Agreement
JS-E-3, Parent/Guardian Opt Out Declaration for Usage of Technology and Internet Resources
JS-E-4, Annual Student Device Technology Fee for Take-Home Devices

LEGAL REFS.:

C.R.S. § 22-16-101, *et seq.* (Student Data Transparency and Security Act)
C.R.S. § 22-87-101, *et seq.* (Children's Internet Protection Act)
C.R.S. § 24-72-204.5 (monitoring electronic communications)
47 U.S.C. § 254(H) (Children's Internet Protection Act)
47 U.S.C. § 231, *et seq.* (Child Online Protection Act)
20 U.S.C §1232g (Family Educational Rights and Privacy Act)