TECHNOLOGY RESOURCES AND INTERNET SAFETY RESPONSIBLE USE FOR STAFF

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. The District believes staff use technology to deliver instruction, enhance productivity, and model appropriate use for other staff and students. 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.

BLOCKING OR FILTERING OBSCENE, PORNOGRAPHIC AND HARMFUL INFORMATION

To protect staff and students from material and information that is obscene, pornographic, or harmful to minors, the District will install technology that blocks or filters such material and information on District computers having Internet or electronic communications access, prior to being issued to staff.

The District reviews and evaluates electronic resources throughout the school year for compliance to Board policies governing the selection of instructional materials.

STAFF MEMBER 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. Staff member use of the Internet, electronic communications and District technology devices is a privilege, not a right. Use digital resources responsibly. Open attachments only from trustworthy sources and be mindful of spam or scams. Email communication should be kept respectful of other users and network resources. 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 willful damage, and may result in disciplinary action and/or legal action. The District may deny, revoke, or suspend access to District technology or close accounts at any time.

Staff members shall review the District's Acceptable Use Agreement and adhere to the expectations stated.

NO EXPECTATION OF PRIVACY

District devices are owned by the District and are intended for educational purposes and District business at all times. Staff members 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

Staff members 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 staff member 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, which 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. Staff members who identify a security problem while using District technology devices must immediately notify a system administrator. Staff members should not demonstrate the problem to other users. Logging on to the Internet or electronic communications as a system administrator is prohibited.

Staff members 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 staff member 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. Staff who elect to use their own device must conform to this and other District policies while the device is using District network/Internet resources. Staff are responsible for keeping devices 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 staff member 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 staff member'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 and staff 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.

CONFIDENTIALITY

Staff members shall not access, receive, transmit or retransmit material regarding students, parents/guardians, District employees or District affairs that is protected by confidentiality laws unless such access, receipt or transmittal is in accordance with their assigned job responsibilities, applicable law, and District policy. It is imperative that staff members who share confidential student information via electronic communications understand the correct use of the technology, so that confidential records are not inadvertently sent or forwarded to the wrong party. Staff members who use email to disclose student records or other confidential student information in a manner inconsistent with applicable law and District policy may be subject to disciplinary action.

If material is not legally protected but is of a confidential or sensitive nature, great care shall be taken to ensure that only those with a "need to know" are allowed access to the material. Staff members shall handle all employee, student, and District records in accordance with applicable District policies.

Disclosure of confidential student records, including disclosure via electronic mail or other telecommunication systems, is governed by state and federal law, including the Family Educational Rights and Privacy Act (FERPA) and the Colorado Student Data Transparency and Security Act.

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.

UNAUTHORIZED CONTENT – SOFTWARE AND APPLICATION PROCESS

The District requires that all software application used on District devices be submitted for testing and approval to appropriate personnel before installation. Staff members 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.

Staff members may choose to use professional judgement with Internet resources without approval and do so at his or her own risk. Staff will hold student data and privacy with the utmost confidentiality.

District 11 incorporates technology designed to report a current list of websites/digital applications accessed and/or used in classrooms on district owned devices. This publicly accessible list captures a reliable measure of usage. The list is updated each semester in accordance with Colorado student data privacy laws.

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, such as Facebook, Instagram, Twitter, etc. Staff members may use social media within District guidelines for instructional purposes, including promoting communications with students, parents/guardians and the community concerning school related activities and for purposes of supplementing classroom instruction. As with any other instructional material, the application/platform and content shall be appropriate to the student's age, understanding and range of knowledge. 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.). The District systems and communication applications have similar functionality and should be considered for integrated use into school community.

REQUESTS FOR ACCESS TO SOCIAL MEDIA SITES

The District understands that online learning includes utilizing constantly changing technology and that many sites that are currently "blocked" by the District's Internet filter may have instructional significance. Requests to make sites accessible for instructional use are reviewed throughout the school year.

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
Revised May 8, 2024

CROSS REFS.: AC, Nondiscrimination/Equal Opportunity
EGAD, Copyright Compliance
GBAA, Employee Sexual and Racial Harassment/Discrimination
JBB Sexual and Racial Harassment/Discrimination Toward 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, Technology Resources and Internet Safety Responsible Use for Students

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)