Boulder Valley School District
File: JS-R
Effective: February 26, 2007
Revised: October 23, 2012, April 23, 2019

STUDENT USE OF THE INTERNET AND ELECTRONIC COMMUNICATIONS

Each student is responsible for their use of technology, whether personal or district-provided. While using district and personal technology resources on or near school property, in school vehicles and at school-sponsored activities, as well as using district technology resources via off-campus remote access, each student must act in an appropriate manner consistent with school, district, and legal guidelines. It is the joint responsibility of school personnel and the parent or guardian of each student to educate the student about his/her responsibilities and to establish expectations when using technology. Use of District technology resources, district provided Internet and use of any form of electronic communication while on the District network are restricted to use for educational purposes only.

Administrators, teachers and staff have a professional responsibility to work together to supervise and monitor students' use of District technology resources in the classroom, 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 will be provided specifically defined objectives and search strategies prior to accessing material and information on the Internet and through electronic communications.

Password Requirements
Students are required to create strong passwords for accessing District technology and email. Requirements for strong passwords include:

1. At least 8 characters in length; and
2. They must satisfy 3 of the 4 following requirements:
    a. At least one upper case character
    b. At least one lower case character
    c. At least one number
    d. At least one special character (a special character is anything other than a letter or number)

Students with both District technology access and email access are required to change their password every 90 days. Students that have District technology access, but no email access are required to change their password every 180 days.

Email Retention
Deleted emails may be purged immediately.

Reporting of Inappropriate content
Students are expected to report to a District staff member any access (their own or that of another student) to material and information that is unsuitable for students as defined by federal and state law and District policy.

Unauthorized and unacceptable use
Because technology and ways of using technology are constantly evolving, every unacceptable use of district District technology 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, or other data:

- 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 educational purposes

- that contains pornographic, obscene or other sexually oriented material or information, either as pictures or writing, or is otherwise inappropriate as defined by state and federal law and District policy

- 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, derogatory, 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 personally identifiable information defined and protected by confidentiality laws including but not limited to the Family Educational Rights and Privacy Act (FERPA) and the Student Data Transparency and Security Act

- that impersonates another individual, group, or organization

Security
Students should not communicate or demonstrate the problem to other users. Utilization of credentials other than those assigned to the user for their own exclusive use is strictly prohibited. Account names or credentials used in the District must not be duplicated or reused for any purpose external to the District. Access privileges are subject to the principle of least privilege; in addition, access to sensitive data may be subject to the requirement of need to know.

Users are strictly prohibited from performing or attempting to perform the following actions:

• gaining unauthorized access to District technology resources, data, networks or systems and by extension, third party data, networks, or systems integrated with the District

• reading, altering, copying, exfiltrating, destroying, or otherwise harming any data outside the user's own authorized scope of access, to include but not limited to, any official file or record of the district or data of another user.

• attacking, destroying, or disrupting the functionality of district technology resources, systems, or networks, including but not limited to denial of service attacks, or the unauthorized alteration of hardware or software

• performing reconnaissance efforts including but not limited to network, system, or vulnerability scanning or any other method utilized to identify or execute security vulnerabilities to obtain unauthorized access to any system or data or for any other purpose.

• reading, altering, or modifying network packets

• exploiting any security vulnerability in an effort to gain unauthorized access accounts, systems or data

• downloading, storing, installing, or utilizing malicious software • deploying or utilizing any malicious hardware

• bypassing or evading security or filtering measures by use of a proxy, virtual private networking, tunneling, or any other method

• employing any type of social engineering effort to gain unauthorized access to District systems, data, or accounts or data of other users

•posting, sharing, or otherwise making available account, system, or network information that would provide access to unauthorized parties, or increase the likelihood of access by unauthorized parties.

• performing any other action that will increase the level of vulnerability, risk, or exposure to threats to District technology resources, networks, systems, or data.

• use of any District technology resource, system, or network performing any of the aforementioned activities against any external network or system used by the District

• students are prohibited from the use of cellular hotspots while on District property with the exception of the event of an emergency or outage which requires use

Any device, application or other technology resource storing or processing data protected by state or federal law or otherwise deemed sensitive in nature by the District must not be left unattended while logged in; devices must employ a configured and enabled lock screen mechanism triggered by a timer, inactivity, or both; and applications must employ an auto-logout mechanism triggered by inactivity.

Students are prohibited from the use of USB or other removable storage devices within the District, or with District technology resources, without the express consent of the District's CIO or designee.

Safety

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

Students must not utilize District technology resources, including any District provided accounts or applications for personal communication, with parties external to the District, unless the use is for educational purposes.

Unauthorized software

Students are prohibited from using or possessing software: (1) that has been downloaded or is otherwise in the user's possession without appropriate registration, licensing, and payment of any fees owed, (2) that has not been approved through the District software approval process, (3) that has been deemed unacceptable by the District, or (4) that otherwise does not comply with District policy or state and federal laws.

End of File: JS-R