Boulder Valley School District
File: JS-R
Effective: February 26, 2007
Revised: October 23, 2012, April 23, 2019, May 26, 2020

STUDENT USE OF TECHNOLOGY

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 when engaging in activity that has an impact on the school community, each student must act in an appropriate manner consistent with School, School District, and legal guidelines. It is the joint responsibility of school personnel and parents and guardians to educate students about their responsibilities and to establish expectations when using technology. Use of District technology resources, including hardware, software, Internet, and use of any form of electronic communication or applications while on the District network, are restricted to use for educational purposes only.

Account and Password Requirements

Account names or credentials used in the District must not be duplicated or reused for any purpose external to the District.

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

Logging Out

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 School 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.

Email Retention

Deleted emails may be purged immediately.

Unauthorized and unacceptable use

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 or transmits through an anonymous remailer
- that accesses fee services without specific permission from the system administrator

Security

Examples of security risks that violate the School District's policies include, but are not limited to, the following:

- using another person's password or any other identifier
- gaining or attempting to gain unauthorized access to School District technology resources, data, networks or systems and by extension, third party data, networks, or systems integrated with the District
- 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
- using or possessing software that has been downloaded without appropriate permissions, has not been approved through the District software approval process, or that otherwise does not comply with School District policy or state and federal laws.
- 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
- bypassing or evading security or filtering measures by use of a proxy, virtual private networking, tunneling, or any other method
- 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.
- using cellular hotspots while on School District property with the exception of the event of an emergency or outage which requires use
- using USB or other removable storage devices within the School District, or with School 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.

End of File: JS-R