Boulder Valley School District
File: GBEE
Adopted: November 27, 2001
Revised: October 23, 2012, August 14, 2018

Associated Regulation: GBEE-R
Associated Exhibits: GBEE-E-1
GBEE-E-2

STAFF USE OF DISTRICT TECHNOLOGY, THE INTERNET AND ELECTRONIC COMMUNICATIONS

The Internet, various forms of electronic communications, and other District technology resources have vast potential to support curriculum and learning. Accordingly, the Board of Education believes these resources should be used in schools as a learning resource to educate and to inform.

The Board of Education supports the use of the Internet, electronic communications, and other District technology 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 Internet and electronic communications are fluid environments in which District staff may access materials and information from many sources. Staff members shall take responsibility to for their own use of District technology resources while on or off of the District network, as well as use of personal devices while connected to the District network, in accordance with this policy. District technology resources must be used only for educational purposes, or to perform assigned job responsibilities.

Filtering:

Web filtering technology that blocks or filters material and information that is unsuitable for students as defined by federal and state law and Board policy shall be deployed by the District. Staff must report access (their own or that of a student or other staff member) to material or information that is unsuitable for students as defined by federal and state law, professes a threat of violence or self harm, or otherwise in violation of this policy, to their supervisor or District administration and the Information Technology service desk.

No expectation of privacy

District technology resources are owned by the District and are intended for educational purposes, District business and performance of assigned job responsibilities at all times. Staff members have no expectation of privacy while using District technology resources. The District reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of District technology resources, including, but not limited to, all Internet, network, application, and electronic communications access and transmission/receipt of materials and information, including such activity on personal devices while connected to the District network. The District reserves the right to utilize and

apply decryption technology such activity within the District (at any time and without prior notice) to the extent allowable by law. All material and information accessed/received through District technology resources shall remain the property of the District.

Public records

Electronic communications sent and received by District staff may be considered a public record subject to public disclosure or inspection under the Colorado Open Records Act. All staff electronic communications shall be monitored to ensure that all public electronic communication records are retained, archived and destroyed in accordance with applicable law and District policy.

Unauthorized and unacceptable uses

Staff members must use District technology resources, as well as personal technology resources while connected to the District network, in a responsible, efficient, ethical and legal manner and in accordance with applicable law and District policy.

Use of District technology resources, systems, and networks for personal gain is prohibited.

Because technology and ways of using technology are constantly evolving, every unacceptable use of District technology 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, 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 education 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, 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

Intentional access or attempt to access material defined above, or defined as unsuitable elsewhere in this policy or in state or federal law, is considered a direct violation of this policy and may subject the staff member to disciplinary action, up to and including termination, and/or criminal or other legal action.

Security

Information security is a high priority for the District. The District is dedicated to adhering to the most current industry standard information security best practices and continuous improvement of its security posture. Staff members who identify abuse, in violation of policy or otherwise, or a security risk or vulnerability while using District technology resources must immediately notify a supervisor, the Information Technology Service desk, and District administration. Staff members must 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 Boulder Valley shall 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 network or system external to District

• staff 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

Staff are prohibited from accessing, storing, or processing data protected by the Family Educational Rights and Privacy Act (FERPA), the Student Data Transparency and Security Act or otherwise deemed sensitive in nature by the District on any device other than that which has been assigned for exclusive use by the staff member, or has been explicitly designated as an administrative or staff use only device.

Staff 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 CIO or designee.

Any device, application or other District technology resource storing or processing data protected by the Family Educational Rights and Privacy Act (FERPA), the Student Data Transparency and Security Act 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 web based applications must employ an auto-logout mechanism triggered by inactivity

Any user identified as a security risk, or as having a history of problems with other technology resources, may be denied access to District systems, networks and other technology.

Confidentiality

Staff members shall not access, receive, transmit or retransmit data or any other material regarding students, parents/guardians, District staff or District affairs that is 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, unless such access, receipt, or transmittal is in accordance with their assigned job responsibilities, applicable law and District policy. In order to maintain data confidentiality and compliance, data subject to confidentiality laws, as well as any other data designated as sensitive by the District, shall employ the use of encryption. It is imperative that staff members who store and share confidential student information in digital form understand how to do so in a safe and secure manner, so that confidential records are not inadvertently shared with the wrong party or made publicly available in any other manner. Staff members who disclose student records or other confidential student information in a manner inconsistent with applicable law and District policy may be subject to disciplinary action, up to termination, and/or criminal or other legal 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.

Data Handling

Storage of District data, in any form, is restricted to District issued technology resources. Staff are prohibited from storing District data, in any form, on personal devices. Storage of District data in unsanctioned external storage providers or applications is strictly prohibited.

Staff members are highly encouraged to configure and utilize multi-factor authentication for any District sanctioned application where data protected by the Family Educational Rights and Privacy Act (FERPA), the Student Data Transparency and Security Act or otherwise deemed sensitive in nature by the District will be stored or processed.

Any device, including but not limited to stationary workstations, mobile devices, permanently attached or approved removable storage, storing or processing data protected by the Family Educational Rights and Privacy Act (FERPA), the Student Data Transparency and Security Act or otherwise deemed sensitive in nature by the District shall employ encryption technology to maintain confidentiality of data.

Staff connecting any personal devices, such as cell phones (including cell phones where a stipend is provided), laptops or tablets, to District sanctioned applications are required to utilize a screen lock mechanism with an automatic screen lock timeout configured.

All District data or data created by District staff while performing their assigned responsibilities, including email, must be securely destroyed when the data no longer maintains value or valid purpose to the District and in accordance with law and the District’s record retention schedule. The District reserves the right to securely reclaim, remove access, or destroy data not meeting value or validity standards (to include email and other electronic communications) at any time and without prior notice.

Use of social media

Staff members may use social media within school 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.

Staff members are prohibited from communicating with students through personal social media platforms/applications. Staff who would like the use social media as an educational tool are required to create and utilize a professional account for exclusive use for District educational purposes.

Online or electronic conduct resulting in a negative impact to the educational environment or other conduct in violation of District policy may form the basis for disciplinary action, up to and including termination, and/or criminal or other legal action.

District-owned Technology Hardware

Staff-issued District technology resources are the sole responsibility of the staff member. Theft, loss, or

damage of all staff-issued hardware devices must be replaced or reimbursed by the staff member, with the exception of theft within a District building where clear evidence is present and a police report has been filed. Staff members must follow Business Services procedures for reporting the incident.

Unauthorized software

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

Staff member use is a privilege

Use of District technology resources and Internet and electronic communications requires personal responsibility and an understanding of and agreement to the acceptable and unacceptable uses of such tools as defined in this policy. Provisioning of District technology resources for use by staff is a privilege, not a right. Availability to and use of District technology resources by staff is contingent upon acceptance of and compliance with this policy. Failure to follow the use procedures and requirements contained in this policy will result in the loss of the privilege to use these tools and restitution for costs associated with damages, and may result in disciplinary action, up to and including termination, and/or criminal or other legal action. The District may deny, revoke or suspend access to District technology or close accounts at any time.

Staff members are required to sign the District's Acceptable Use Agreement before technology resource accounts will be issued or access allowed utilizing District owned devices. Staff will be prompted with and must accept this agreement while connecting to the District network with their personal devices.

School District makes no warranties

The District makes no warranties of any kind, whether express or implied, related to the use of District technology resources, 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 or quality of information. The District is not responsible for any damages, losses or costs a staff member or student suffers in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via District technology resources is at the staff member’s own risk.

Definition:

As used in this policy, the terms “staff,” “staff member” and “District staff” include any person employed by the District, student teachers, interns, volunteers, contractors, or any other third party under contract to perform work or services or process data for the District.

LEGAL REFS.: 47 U.S.C. 254(h) (Children's Internet Protection Act of 2000)
47 U.S.C. 231 et seq. (Child Online Protection Act of 2000)
20 U.S.C. 6801 et seq. (Elementary and Secondary Education Act)
C.R.S. 22-87-101 et seq. (Children's Internet Protection Act)
C.R.S. 24-72-204.5 (monitoring electronic communications)

End of File: GBEE