Superintendent File: GBEE

STAFF USE OF DISTRICT INFORMATION TECHNOLOGY

The District provides technology ("District IT") to support the educational mission of the District and its schools and to enhance the curriculum and learning opportunities for students and school staff.

For purposes of this policy, "District IT" means any District-owned service, network, computer, hardware, software, artificial intelligence, e-mail account, or other technology, that is used to support the educational mission or business purposes of the District.

"Artificial intelligence" means a set of technologies that enable computers or devices to perform a variety of advanced functions, including the ability to see, understand and translate spoken and written language, analyze data, make recommendations, among other tasks. These technologies can form the basis of platforms that generate video, audio, and textual results (e.g., Khanmigo, ChatGPT, Gemini, Claude, et al).

The Internet and electronic communications are fluid environments in which users may access materials and information from many sources. Staff members shall take responsibility for their own use of District IT to avoid contact with material or information that violates this policy.

The intent of this policy is to provide staff members with general requirements for utilizing the District IT , including electronic communications. The superintendent or designee may supplement this policy with more specific administrative regulations governing day-to-day management and operation of the District IT and electronic communications. The superintendent may delegate specific responsibilities to building principals and others as deemed appropriate.

This policy provides general guidelines and examples of prohibited uses for illustrative purposes, but does not attempt to state all required or prohibited activities by users. Staff members who have questions regarding whether a particular activity or use is acceptable should seek further guidance from their principal or appropriate administrator.

Access to District IT

The level of access that staff members have to District IT is based upon specific job requirements and needs.

Acceptable use

Staff member access to the District IT is provided to support the educational mission or business purposes of the District. General rules and expectations for professional behavior and communication apply to the use of the District IT. Staff members shall use District IT in a responsible, efficient, ethical and legal manner.

Prohibited use

Staff members are responsible for their actions and activities involving District IT, and for computer files, passwords and accounts.

General examples of unacceptable uses that are expressly prohibited include, but are not limited to, the following:

1. Any use that is illegal or in violation of Board or District policies, including harassing, discriminatory, or threatening communications and behavior; violations of copyright laws or trade secrets; or use of software without proof of proper licensing;

2. Any use involving materials that are obscene, pornographic, sexually explicit, or sexually suggestive;

3. Any inappropriate communications with students or minors;

4. Any use for private financial gain, or commercial, advertising, or solicitation purposes;

5. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate, or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school sponsored organization; to raise funds for any non-school sponsored purpose, whether profit or non-for-profit; or to engage in political activities or campaigns. Staff members who are uncertain as to whether particular activities are acceptable should seek further guidance from their building principal or other appropriate administrator;

6. Any communication that represents personal views as those of the school or District or that could be misinterpreted as such;

7. Downloading or loading software or applications without permission from the system administrator;

8. Opening or forwarding any e-mail attachments (executable files) from unknown sources and/or that may contain viruses;

9. Sending mass e-mails to school users or outside parties for school or non-school purposes without the permission of the system administrator, principal, or designated administrator;

10. Any malicious use or disruption of District IT or breach of security features;

11. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct;

12. Any attempt to access unauthorized sites;

13. Failing to report a known breach of computer security to the system administrator;

14. Using District IT after such access has been denied or revoked; and

15. Any attempt to delete, erase, or otherwise conceal any information stored on District IT in violation of policy, applicable law or district direction.

Blocking or filtering obscene, pornographic and harmful information

To protect students from material and information that is obscene, pornographic or otherwise harmful to minors, as defined by the District, technology that blocks or filters such material and information has been installed on all District computers having Internet or electronic communications access. Blocking or filtering technology may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by staff members over the age of 18.

No expectation of privacy

District IT is owned by the District and is intended for educational purposes and District business at all times. Staff members have no expectation of privacy in their use of District IT , including e-mail messages and stored files. The District retains control, custody, and supervision of all District IT owned or leased by the District. The District reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of District IT, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through District IT shall remain the property of the District.

Public records

Electronic communications sent and received by District staff members may be considered a public record subject to public disclosure or inspection under the Colorado Open Records Act.

Security

Security on District IT is a high priority. Staff members who identify a security problem while using District IT 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 IT
- 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 District IT.

Confidentiality

Staff members shall not access, receive, transmit or retransmit material regarding students, parents/guardians, District staff members 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).

Use of social media

Staff members may use social media within District guidelines for instructional purposes, including promoting communications with groups of 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 discouraged from communicating with students through personal social media platforms/applications or texting. Staff members are expected to protect the health, safety and emotional well-being of students and to preserve the integrity of the learning environment. Online or electronic conduct that distracts or disrupts the learning environment or other conduct in violation of this or related District policies may form the basis for disciplinary action up to and including termination.

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 operation of any network within the District or any network connected to the Internet, 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

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 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 IT is a privilege, not a right. 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 action. The District may deny, revoke or suspend access to District technology or close accounts at any time.

Staff member acknowledgement required

Each staff member authorized to access the District IT is required to sign an acknowledgement form stating that the staff member has read this policy. The acknowledgement form will be retained in the staff member's personnel file.

District makes no warranties

The District makes no warranties of any kind, whether expressed or implied, related to the use of District IT, 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 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.

Adopted: May 7, 2002
Revised by the Superintendent: August 5, 2003
Revised: August 28, 2006
Revised by the Superintendent**:** December 10, 2020
Revised: October 9, 2024

LEGAL REFS.:

20 U.S.C. 6751 *et seq. (Enhancing Education Through Technology Act of 2001)*
47 U.S.C. 254(h) *(Children's Internet Protection Act of 2000)*
47 C.F.R. Part 54, Subpart F *(Universal Support for Schools and Libraries)*
C.R.S. 22-87-101 *et seq. (Children's Internet Protection Act)*
C.R.S. 24-72-204.5 *(monitoring electronic communications)*

CROSS REFS.:

AC, Nondiscrimination/Equal Opportunity
GBEB
GBEE-R
EGAEA, Electronic Communication