

GBEF-R

REGULATION

USE OF PORTABLE WIRELESS COMMUNICATIONS AND DEVICES

Safe and Appropriate Use of Technology

Technology must be used in a responsible, efficient, ethical, and legal manner and in accordance with District policies and educational goals. This regulation provides guidance to District employees and other authorized users in their use of the District's Electronic Information Services (including computer systems, networks, and other technology resources). It also establishes expectations for the use of digital communications and electronic devices for District-related purposes, whether or not the devices are District-owned or connected to the District's Electronic Information Services.

Acceptable Use of the District's Electronic Information Services (EIS)

The use of the District's EIS is a privilege and not a right. Individual access to the District's EIS shall be by authorization only. Designated personnel may provide authorization to staff who have completed and returned an annual Acceptable Use Agreement. The Superintendent may give authorization to other persons to use the District's EIS. Employees leaving the District shall discontinue use of District technology upon termination of employment. Access to the District's EIS will be removed.

The following sets out rules for District employees to follow to appropriately use the District's EIS. Each user of the District's EIS, including a user of a Personal Electronic Device (PD) shall:

- A. Use the District's EIS to support educational objectives consistent with the educational goals and objectives of the District. District internet and property may only be used for authorized activities.
- B. Abide by all copyright and trademark laws and regulations.
- C. Understand that electronic mail or direct electronic communication is not private and may be read and monitored by the District.
- D. Use electronic mail only for communications that are relevant and of interest to mail recipients.
- E. Observe all applicable state or federal laws.
- F. Obtain permission to record, transmit, or post photos or a video of a

person with any electronic device.

G. Obtain permission from a classroom teacher or an administrator before making publicly available any images, video, or audio files recorded at school during school hours or at any school-sponsored event or activity, regardless of the time or location.

H. Understand that inappropriate use may result in cancellation of permission to use the District's EIS and appropriate disciplinary action.

I. Understand that many services and products are available for a fee and acknowledge personal responsibility for any expenses incurred without District authorization.

J. Use the District-created alias as the only form of masked identity when using the District's EIS.

K. Maintain supervision of students using the District's EIS, including use of PDs.

L. Take responsibility for the content of their posting on any form of technology through any form of communication.

M. Take responsibility for assigned personal and District accounts, including password protection.

N. Take all responsible precautions, including password maintenance and file and directory protection measures, to prevent the use of personal and District accounts and files by unauthorized persons.

O. Adhere to all District policies related to technology, including but not limited to, the use of District technology, copyright and trademark laws, student rights, parent rights, the Family Educational Rights and Privacy Act (FERPA), staff ethics, mandatory reporting requirements, and staff-student relations.

The following includes prohibited uses of the District's EIS. Each user of the District's EIS, including a user of a PD, shall not:

A. Send, submit, publish, display, or retrieve any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, intimidating, fraudulent, or illegal material.

B. Use the network in any way that would disrupt the use of the network by others.

C. Use the District's EIS for commercial purposes, or personal financial gain, or to solicit funds, donations, purchases, or other support for non-District purposes or causes, including but not limited to, operating or promoting a private business, selling goods or services, conducting outside employment, or soliciting contributions to or participation in charitable fundraisers.

D. Attempt to harm, modify, add or destroy software or hardware nor interfere with system security.

E. Disclose home addresses, personal phone numbers or personally identifiable data unless authorized to do so by designated school authorities.

F. Attempt to log into the District's EIS using any account and/or password other than the login(s) assigned to the user.

Violation of the rules set out above and/or a law, District policy, procedure, or school rule related to technology use will result in staff discipline in accordance with state law, Board policies and regulations, and the District Code of Conduct.

It shall be the responsibility of all District employees to be knowledgeable of the details of the Acceptable Use Agreement. When the signed agreement is returned to the school, the user may be permitted use of the District's EIS resources through the school equipment.

The District reserves the right to enact rules and regulations essential for the efficient administration of the electronic information systems.

Duty Not to Waste District Resources

Users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to sending mass mailings, printing multiple copies of documents, downloading lengthy files such as non-educational games, movies and music, streaming music or movies, or otherwise creating unnecessary network traffic.

Content Filtering

A content filtering program or similar technology shall be used on the District's networked EIS as well as on standalone computers capable of District authorized access to the Internet. The technology shall at a minimum limit access to obscene, profane, sexually oriented, harmful, or illegal materials. Should a District adult employee have a legitimate need to obtain information from an access-limited site, the Superintendent may authorize, on a limited basis, access for the necessary purpose specified by the employee's request to be granted access.

Installation of Software

Employees may not install personal software onto District computers without first receiving the express permission of their administrator and the Director of Educational Technology. Employees requesting permission to install personal software must provide the administrator with a copy of the software

license that permits them to install the software. Files obtained from sources outside the District, including electronic storage devices brought from home and files downloaded from newsgroups or bulletin boards, may contain dangerous computer viruses and should never be downloaded onto District computers without prior approval. This is not intended to restrict the downloading of files from Internet sources or online services for use as curriculum supplements by teachers.

Personal Electronic Devices (PDs)

The District's goal is to increase access to digital tools and facilitate more immediate access to technology-based information. To this end, the District recognizes the value of allowing staff to bring their own personal devices (PDs) to school to connect to the District's EIS. The purpose of this section is to authorize and establish reasonable rules for staff to possess and use their PDs at school.

A PD is any electronic device owned by a staff member that stores, transmits, receives or displays voice messages, data, or images, or provides a wireless unfiltered connection to the Internet. This definition includes, but is not limited to, cellular telephones, digital audio players, digital cameras, laptop computers, tablet computers, pagers, portable game players, smartwatches, smart glasses, and any new technology developed with similar capabilities.

This regulation applies to a staff member's use of a PD while 1) on school property, 2) at a school event held on school property, or 3) while using the District's network (including at home).

- A. A staff member is permitted to use a PD only after the staff member has signed and returned the annual Acceptable Use Agreement.
- B. Employees shall not use personal cellular service or another external Internet service to circumvent District network filtering, security measures, or access restrictions, or to access, display, share, or otherwise use instructional materials or resources with students.
- C. Staff do not have any expectation of privacy in anything they create, store, send, receive, or display on or over the District's EIS.
- D. On school property, a staff member may not use a PD to connect to the District's network by a network cable plugged into a data outlet. Also, on school property, a staff member may not print from a PD.
- E. The District is not liable for any PD that is lost, damaged, or stolen. Each staff member is responsible for their own PD, including set-up, maintenance, charging, and security.
- F. The District is not responsible for the payment of any user fees or data charges associated with the use of a PD that are billed by a third party even if the fees or charges were incurred for an educational

purpose.

*Acceptable Staff Use of
Digital Communications and
Electronic Devices*

Employees are encouraged to appropriately and responsibly use digital communications and electronic devices to support learning, collaboration, communication, and relationship building. Because technologies and methods of digital communication continue to evolve, the District will review these guidelines annually to ensure they remain current, relevant, and responsive to District needs.

The PAT Test

Employees should apply the *Professional, Accessible, and Transparent (PAT) Test* when using electronic communication tools for district-related purposes. Electronic communication with colleagues, students, and parents/legal guardians should be professional, accessible, and transparent as described below.

Professional: Electronic communication should reflect the employee's professional role and responsibilities. Word choice, tone, content, and subject matter should be appropriate for a professional school environment and consistent with district expectations for respectful and responsible conduct.

Accessible: Employees should communicate with the understanding that district-related electronic communications may be retained, reviewed, accessed by others, or subject to disclosure in accordance with applicable law and district policy.

Transparent: District-related electronic communication should be open and appropriate for a professional school setting. Employees should communicate in ways that support visibility, accountability, and appropriate oversight.

District-Approved
Communication Methods

The list below outlines district-approved communication methods for contacting students and parents/legal guardians:

- District e-mail
- District phone
- District website
- School website

- School-related social media
- ParentSquare
- District student information system (Synergy)
- District-approved applications, such as Google Classroom

These communication methods are approved for District-related communications because they are monitored by the District, and conform to District-set parameters, filters, and firewalls. Messages and information using these tools can be monitored by the District, are retrievable, and may be produced as documentation, if required.

Employees are expected to follow District policies, regulations, and always protect student confidentiality and rights to privacy. Third-party communication applications, including but not limited to Band, Strava, WeChat, WhatsApp, and similar applications are not approved for communicating with students or parents/legal guardians and may not be used for such communications.

Use of Social Media by District Employees

In this regulation, the term "school-related social media" means use of District-approved social media through the District's EIS. The term "personal social media" means all other use of social media, including an individual's own private and/or commercial use of social media, not connected to the District's EIS. The term "communication" includes words, pictures, drawings, photographs/images, and videos.

Use of School-Related Social Media by District Employees

The District recognizes that social media can support communication, collaboration, professional learning, and engagement with the school community. Employees who use social media in connection with their professional responsibilities are expected to exercise sound judgment and maintain appropriate professional boundaries.

The following guidelines are intended to help employees use school-related social media responsibly and in a manner consistent with District policies and professional expectations.

- A. Communications with other employees, individual students, parents/legal guardians, and other members of the school community must always be professional in content and tone.
- B. An employee shall report disrespectful, defamatory, discriminating, harassing, intimidating, bullying, vulgar and/or obscene behavior as well as questionable conduct, contact, or content to a school

administrator.

- C. Confidential or private information about students, employees, parents/legal guardians, or other members of the school community shall not be disclosed by employees.
- D. All social media communications using the District's EIS may be monitored by the District.
- E. Communications with students shall be academic in nature and relate to school topics. Employees shall avoid discussion of personal topics with students.
- F. Employees shall ensure that their profile and related social media site are professional and consistent with how they wish to present themselves publicly and should not reflect negatively on the employee or the District.
- G. An employee shall use their real name and always be identifiable as an employee of the District.
- H. The District's proprietary content and information (e.g., District assessments, curriculum, etc.) shall not be shared. Employees shall comply with copyright laws when using the creative works of others.
- I. Employees shall limit exposure of advertising to students and families.
- J. Employees shall follow the law, Board policies, and District regulations. Read and follow the "Terms of Service" of providers and, for teachers, ensure that students do the same.
- K. Employees who wish to create a social media account associated with the District, a school, a classroom, or any other District-affiliated organization must be granted approval by site and District administration. Employees who create or maintain social media accounts as part of their job must agree to the following:
 - a. The employee must read and understand the social media guidelines for employees outlined in Policy GBEF and this regulation.
 - b. Before posting student photos, the employee must verify the media release status of each student.
 - c. The employee must acknowledge that they are solely responsible for managing the information and posts on the page.
 - d. The employee must agree to add the site principal and District personnel as administrators on the page or provide the site principal and District personnel with the username and password for the account.
 - e. The employee must agree to allow District personnel to manage

privacy settings and assist if necessary.

Web Publishing

The District recognizes the value and potential of publishing on the Internet. School faculty and staff may create electronic home pages or group pages that seek to carry out official business and communication of the District's mission. All such pages must be accessible to the District, the parent/legal guardian, and students from an official school website within the District. All staff publishers must adhere to the policies of the District and must comply with all relevant federal and state laws. Web pages shall not display personally identifiable student information unless explicit and verifiable written permission has been granted by the student's parent/legal guardian. Web pages must comply with District policies and professional expectations. E-mail addresses/links on web pages must be a *cfsd16.org* address. The District provides computer services and networking to enhance the District's educational and administrative processes, and to improve communication with the world community. Material that fails to meet established educational objectives or that is in violation of a provision of District policy and administrative regulations will be removed.

Use of Personal Social Media by District Employees:

The following guidelines are intended to help District employees use personal social media responsibly and in a manner consistent with District policies and professional expectations.

- A. *Employees using personal social media to communicate with friends, family, and personal networks are encouraged to have privacy settings in place. Employees may not use their District e-mail or phone number for communications on social media networks for personal accounts.*
- B. *When private information from a personal social media account is disclosed to the District, it may be investigated.*
- C. *Employees are required to maintain a professional relationship with students.*
 - a. *To maintain this professional relationship, employees shall not "friend" or accept social media requests from students. Employees shall redirect students to school-related social media sites approved by the District.*
 - b. *The only exception is that, with administrative approval, an employee may use personal social media to communicate with a student who is a relative or a close family friend.*
- D. *An employee shall not communicate in a manner that is unprofessional and would 1) disclose confidential or private information; 2) cause harm to students, parents/legal guardians, employees, or other members of the school community; 3) significantly and adversely impact the*

employee's work-related reputation or the reputation of the District; 4) reflect negatively on the employee, a colleague, student, or the District. These restrictions shall not be interpreted to prohibit any communication on a matter of public concern when the employee's interest in engaging in the communication outweighs the District's interest in managing its workforce effectively.

Employees with questions about appropriate school-related or personal social media boundaries should consult their principal, supervisor, or Human Resources.