

**GBEF
STAFF USE OF DIGITAL COMMUNICATIONS
AND ELECTRONIC DEVICES**

The Governing Board recognizes how web-based and mobile technologies are fundamentally changing opportunities to communicate with individuals or groups and how their use can empower the user and enhance discourse. The Board equally recognizes that the misuse of such technologies can be potentially damaging to the District, employees, students and the community. Accordingly, the Governing Board requires all employees to adhere to adopted policies and to utilize digital communications and electronic devices in a professional manner at all times.

The Board establishes the following parameters:

District employees

- A. shall adhere to all Governing Board policies related to technologies including but not limited to the use of District technology, copyright laws, student rights, parent rights, the Family Educational Rights and Privacy Act (FERPA), staff ethics, and staff-student relations;
- B. are responsible for the content of their posting on any form of technology through any form of communication;
- C. shall only use District approved technologies when communicating with students or parents;
- D. shall not use District owned or provided technologies to endorse or promote a product, a cause or a political position or candidate;
- E. in all instances must be aware of his/her association with the District and ensure the related content of any posting is consistent with how they wish to present themselves to colleagues, community members, parents and students;
- F. shall not use District logos or District intellectual property without the written approval of the Superintendent;
- G. shall use technologies to enhance and add value to communications with all recipients and be respectful of those with whom they communicate;
- H. shall immediately report all misuse or suspected misuse of technology to their direct supervisor/administrator who in turn will immediately report to the Superintendent;
- I. shall comply with all applicable records management parameters established by Arizona State Library, Archives and Public Records.

The Superintendent shall communicate the above to all employees of the District at the beginning of each school year and to newly hired employees as part of the hiring process.

The Superintendent shall establish which technologies are approved for use by employees to communicate with parents and students. Approved technologies shall be communicated to the Board and employees prior to the start of every school year, to newly elected Board members prior to taking office, and to newly hired employees as part of the hiring process.

The Superintendent shall determine which records retention and management guidelines as established by the Arizona State Library, Archives and Public Records are applicable to this Board policy and communicate these guidelines to the Board and employees prior to the start of every school year, to newly elected Board members prior to taking office, and newly hired employees as part of the hiring process.

Violations of this policy may result in disciplinary action up to and including termination and may constitute a violation of federal or state law in which case appropriate law enforcement shall be notified. The Superintendent shall report violations of this policy to the Board and shall make reports to the appropriate law enforcement agency when determined necessary.

Adopted: October 9, 2018

LEGAL REF.:

A.R.S.

15-341

15-514

CROSS REF.:

GBEA - Staff Ethics

GBEB - Staff Conduct

GBEBB - Staff Conduct With Students

GCQF - Discipline, Suspension, and Dismissal of Professional Staff Members

GDQD - Discipline, Suspension, and Dismissal of Support Staff Members

IJNDB - Use of Technology Resources in Instruction

JIC - Student Conduct

GBEF-R

REGULATION

STAFF USE OF DIGITAL COMMUNICATIONS AND ELECTRONIC DEVICES

Introduction

Employees are encouraged to use electronic communications to appropriately and responsibly participate in this rapidly growing environment of learning, collaboration, and relationship building. In light of ever-evolving technologies and online social tools, the District will review these guidelines annually to ensure they remain current to our needs.

The TAP Test

Employees should apply the Transparent, Accessible, and Professional (TAP) Test to all online tools and messages used on those tools. Electronic communication with one another, with students, and with parents should always be transparent, accessible, and professional, as defined below:

Transparent: Electronic communication between staff, students, and parents should be transparent. As a public school district, we are expected to maintain openness, visibility, and accountability with regard to all communications.

Accessible: Electronic communication between staff, students, and parents is a matter of public record and/or may be accessible by others.

Professional: All electronic communication from staff to student or parent should be written as a professional representing the Flowing Wells Unified School District (FWUSD). This includes word choice, tone, grammar, and subject matter that model the standards and integrity of a professional educator. Always choose words that are courteous, conscientious, and generally businesslike in manner.

Before hitting "send" or "post" consider this question, "Would I mind if this information appeared on the front page of the local newspaper?" Please remember that e-mail and social networking are very public places.

Encouraged Communication Methods:

- District E-mail
- District Phone
- District Website

- School Website
- District Student Database
- District-Approved Applications, such as Google Classroom and Edmodo

These communication methods are always acceptable 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, just as though writing a letter or having a face-to-face conversation.

Use Caution Communication Methods:

- "Friending" parents - check privacy settings
- Contacting parents using personal phones

Use Extreme Caution Communication Methods:

- Personal social media for any contact with students or parents
- "Friending or following" students, or accepting friend or follow requests from students.
- Personal to personal e-mail
- Texting students/parents
- Calling students using personal phones

If planning to use a communication method from the "Use Caution" or "Use Extreme Caution" category, *the employee must:*

- Consult with the principal or supervisor to discuss how the tool will be used and to obtain approval.
- Contact the parents and document their consent for the student to participate.
- Have an opt-out option and a viable alternative for the student to participate.

Unacceptable Communications Methods:

- *Online Games and Related Activities.* While many people enjoy a variety of gaming systems (Wii, Xbox, etc.) and recreational websites that allow them to compete with others through the Internet, this is not an acceptable activity for staff members to engage in with students.

Bring Your Own Device (BYOD):

- The District's goal is to increase students' access to digital tools and facilitate more immediate access to technology-based information, much in the way students utilize pen and paper. To this end, the District recognizes the value of allowing students to bring their own devices to school to connect to the District's electronic information systems (EIS). These devices are commonly referred to as Bring Your Own Device (BYOD) or personal electronic devices (PDs). The purpose of this section is to authorize and establish reasonable rules for students to possess and use their PDs at school.
- A PD is any electronic device owned by a student or his/her family that stores, transmits, receives or displays voice messages, data, or images, or provides a wireless unfiltered connection to the Internet.
- This regulation applies to a student's use of a PD while 1) on school property (including buses), 2) at a school event, or 3) while using the District's network (including at home).
- A student is permitted to use a PD only after the student and a parent/guardian have signed and returned the annual Acceptable Use Agreement.
- In a classroom setting, a student may only use a PD for educational purposes at the direction of a teacher or administrator. Other than in a classroom setting on school property, the administration at each school will determine where and when and for what purpose a student may use a PD. A school administrator or staff member always has the right to prohibit a student(s) from using a PD at certain times or during designated activities that occur during the school day (e.g., school presentations/assemblies, theatrical performances, or guest speakers).
- In a classroom setting, a student is prohibited from using a PD to access the Internet using any external Internet service (e.g., cellular connections and mobile hot spots). In a classroom setting, a student using a PD, including a smart phone, may only access the Internet using the Wi-Fi access provided by the District.
- The student/owner of a PD is the only person allowed to use the device. Students are prohibited from sharing their assigned user name and/or password with others. A student must sign in to the designated PD District wireless network using his or her assigned username and password.

- If a student's use of a PD causes disruption in any setting, the student can be directed either to put the PD away and/or the PD can be confiscated and the student referred to an administrator for further discipline.
- On school property, a student may not use a PD to connect to the District's network by a network cable plugged into a data outlet.
- The District is not liable for any PD that is lost, loaned, damaged, or stolen. Each student is responsible for his or her own PD, including set-up, maintenance, charging, and security. Staff members will not store a student's PD, nor will any District staff be expected to diagnose, repair, or work on any PD. If a PD breaks while being used in school, the student should put the device away and take it home at the end of the school day where the student and the parent/guardian can troubleshoot the issue.
- 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 to a student and/or a student's parent/guardian, even if the fees or charges were incurred by the student for an educational purpose.
- A student who violates a law, District policy, procedure, or school rule while using a PD will be disciplined pursuant to District policies. In addition, an administrator can revoke a student's PD privileges.
- Students do not have any expectation of privacy in anything they create, store, send, receive, or display on or over the District's EIS.
- School officials may search and/or seize a student's PD if there are reasonable grounds for suspecting that the search or seizure will reveal evidence that the student has violated or is violating the law or a District policy, procedure, or school rule.
- PDs are a supplement to the equipment already in use in the classroom. BYOD is an optional program and parents are not required to purchase a device for their child. Students who do not have access to a PD will be provided with comparable District-owned equipment for classroom lessons that require access to technological resources. Access to or use of PDs will not be used as a factor in grading or assessing student work.

Important Reminders

Employees should be aware that e-mailing, texting, and other electronic communications between a staff member and student could be easily misinterpreted by a student or parent. If an employee or coach plans to send electronic communications a student's phone for immediate and urgent contact with students or team members, the employee or coach must be transparent about such use.

Make the parents aware at the beginning of the school year or season that you will be e-mailing or texting.

Social media sites for personal purposes. Employees using Facebook to communicate with friends, family, and personal networks should ensure their privacy settings are set to "Friends." If the "Friends of Friends" or "Everyone" settings are used, employees open their content to a much larger group of people, including students and parents. Employees using Instagram should set their accounts to "Private." Employees using Twitter should change settings to approve follower requests. Employees should not use their District e-mail or phone number for communications on social media networks for personal accounts.

The wall between public educator and personal friend with students should always be visible and strongly communicated. Please talk to your principal/supervisor or human resources if you have any questions or concerns.

Creating or Maintenance of a Social Media Account Associated with a Classroom, School, or the District

Employees who wish to create a social media account associated with the District must complete the Flowing Wells Social Media Application form and be granted approval by site and District administration. Employees who create or maintain social media accounts as part of their job in Flowing Wells must agree to the following:

- The employee must read and understand the social media guidelines for employees outlined in Policy GBEF and this regulation.
- Before posting student photos, the employee must verify the media release status of each student.
- The employee must acknowledge that he/she is solely responsible for managing the information and posts on the page.
- 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.
- The employee must agree to allow District personnel to manage privacy settings and assist if necessary.