



TEXARKANA
Independent School District

**TECHNOLOGY
ACCEPTABLE USE PROCEDURE
2026-2027**

Procedure

Acceptable Use

The district's technology resources will be used for learning, teaching, and administrative purposes consistent with the district's mission and goals.

Improper Use Includes:

- Submitting, publishing or displaying any defamatory, cyberbullying, inaccurate, racially offensive, abusive, obscene, profane, sexually-oriented, or threatening materials or messages either public or private;
- Attempting to or physically damaging equipment, materials or data;
- Attempting to or sending anonymous messages of any kind, except as expressly allowed by the District's Elevate system;
- Pretending to be someone else when sending/receiving messages;
- Using District resources for personal and commercial use;
- Using the network to access inappropriate material;
- Knowingly placing a computer virus on a computer or the network;
- Opening email messages from unknown senders, loading data from unprotected computers, and any other risky action that may introduce viruses to the system;
- Accessing technology resources, files, and documents of another user without authorization;
- Attempting to or using proxy servers or otherwise bypassing security to gain access to the Internet or network resources;
- Posting personal information about others without proper authorization;
- Attempting to "hack" into technology resources;
- Storing non-work-related information (i.e. programs,.exe files, non-work-related videos) on the district's storage systems;
- Attempts to degrade or disrupt resource performance including but not limited to denial-of-service attacks;
- Any interference with the work of others, with or without malicious intent;
- Forgery or attempted forgery of electronic messages or data;
- Violation of copyright laws; Installing software without proper approval;
- Installing or setting up any device that would alter the network topology including wireless access points, routers, hubs, or switches;
- Inappropriate desktop backgrounds and screensavers;
- Attempting to gain unauthorized access to third party networks or systems through the use of District resources;
- Giving your Password or Account Access to anyone - including your own family;
- Setting up a Wi-Fi Hotspot in order to circumvent district wireless settings to bypass the district internet filtering.

Network Access

Access to the District's network systems will be governed as follows:

- Your user account is your own. Do not share your username or password, even with other staff or students.
- You are required to keep your password confidential. It is important to remember that your password allows access to multiple systems, and many of those systems contain FERPA protected information.
- Make sure not to store any passwords in easily accessed locations.
- Do not allow another person to use your account to access Texarkana ISD wireless networks or to log into desktops.
- Any system user identified as a security risk or having violated the Technology Acceptable Use Policy may have their access privileges revoked to the district's system. Other consequences may also be administered.
- You are responsible for all actions taken by your user account.
- The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District guidelines.
- For information on accessing the Texarkana ISD wireless network consult the: [Texarkana ISD - Wireless Network Reference](#)

Suspension or Termination of a Network User Account

The district may suspend or terminate a user's access to the district's system upon suspected violation of District policy and/or administrative regulations regarding acceptable use. A user's account will always be disabled once they leave the district's employment.

Data Security

As part of your duties, you may have access to confidential information. Caution must be taken to ensure this data is not exposed to those without a need to know. A data file containing confidential information that is released can damage the financial or professional futures of others, thus this information must be handled appropriately.

- Limit data exports to only the necessary information on the required people.
- Do not leave data files or computer equipment in an unsecured location such as an unattended automobile.
- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone from their office. This information should be kept in a locked drawer when the desk is unoccupied.
- Printouts containing confidential information should be immediately removed from the printer. Upon disposal, confidential information should be shredded using District shredders.
- Whiteboards, etc. containing sensitive information should be erased after use.
- Lock up portable computing devices including laptops, external drives, and flash drives.
- Access to confidential information should be given on an as-needed basis. If you are able to access confidential information that you do not need, you are required to report it to the manager of that data system.
- Be very cautious in transporting data files. Data transported on flash drives or external drives can be lost easily.
- Cloud-based storage systems like Google Drive are susceptible to leaks especially if users do not correctly configure sharing permissions. Staff should keep in mind what data should be kept confidential when sharing any files or folders with contacts outside the district.
- Confidential information sent via Gmail should always have confidential mode enabled. This feature should be used for all confidential email, including internal District communication.
- Data files containing confidential information that are leaving the district via email or on media should be encrypted (contact the Technology Department for assistance).

Personal Use of Electronic Communications

(Policies CQ, CY, DHA)

Electronic communications include all forms of social media, such as text messaging, instant messaging, electronic mail (email), web logs (blogs), wikis, electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, X, LinkedIn, Instagram). Electronic communications also include all forms of telecommunication such as landlines, cell phones, and web-based applications.

As role models for the district's students, employees are responsible for their public conduct even when they are not acting as district employees. Employees will be held to the same professional standards in their public use of electronic communications as they are for any other public conduct. If an employee's use of electronic communications interferes with the employee's ability to effectively perform his or her job duties, the employee is subject to disciplinary action, up to and including termination of employment. If an employee wishes to use a social network site or similar media for personal purposes, the employee is responsible for the content on the employee's page, including content added by the employee, the employee's friends, or members of the public who can access the employee's page, and for web links on the employee's page. The employee is also responsible for maintaining privacy settings appropriate to the content.

An employee who uses electronic communications for personal purposes shall observe the following:

- The employee may not set up or update the employee's personal social network page(s) using the district's computers, network, or equipment.
- The employee shall limit use of personal electronic communication devices to send or receive calls, text messages, pictures, and videos to breaks, mealtimes, and before and after scheduled work hours, unless there is an emergency or the use is authorized by a supervisor to conduct district business.

- The employee shall not use district and campus trademarks, including names, logos, mascots and symbols or other copyrighted material on social media or in texts without express written consent.
- An employee may not share or post, in any format, information, videos, or pictures obtained while on duty or on district business unless the employee first obtains written approval from the employee's immediate supervisor. Employees should be cognizant that they have access to information and images that, if transmitted to the public, could violate privacy concerns.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Texas Educators' Code of Ethics, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off campus. These restrictions include:
 - Confidentiality of student records. (See Policy FL)
 - Confidentiality of health or personnel information concerning colleagues, unless disclosure serves lawful professional purposes or is required by law. (See Policy DHA (LEGAL))
 - Confidentiality of district records, including educator evaluations and private email addresses. (See Policy GBA)
 - Copyright law (See Policy CY)
 - Prohibition against harming others by knowingly making false statements about a colleague or the school system. (See DHA(LEGAL))

See *Electronic Communications between Employees, Students, and Parents*, below, for regulations on employee communication with students through electronic media.

Electronic Communications between Employees, Students, and Parents

(Policy DH)

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may use electronic communications with students who are currently enrolled in the district. The employee must comply with the provisions outlined below. Electronic communication between all other employees and students who are enrolled in the district is prohibited.

Employees are not required to provide students with their personal phone number or email address.

An employee is not subject to the provisions regarding electronic communications with a student to the extent the employee has a social or family relationship with a student. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization. An employee who claims an exception based on a social relationship shall provide written consent from the student's parent. The written consent shall include an acknowledgement by the parent that:

- The employee has provided the parent with a copy of this protocol;
- The employee and the student have a social relationship outside of school;
- The parent understands that the employee's communications with the student are excepted from district regulation; and
- The parent is solely responsible for monitoring electronic communications between the employee and the student.

The following definitions apply for the use of electronic media with students:

- *Electronic communications* mean any communication facilitated by the use of any electronic device, including a telephone, cellular telephone, computer, computer network, personal data assistant, or pager. The term includes email, text messages, instant messages, and any communication made through an Internet website, including a social media website or a social networking website.
- *Communicate* means to convey information and includes one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not a *communication*; however, the employee may be subject to district regulations on personal electronic communications. See *Personal Use of Electronic Communications*, above. Unsolicited contact from a student through electronic means is not a *communication*.

- *Certified or licensed employee* means a person employed in a position requiring SBEC certification or a professional license, and whose job duties may require the employee to communicate electronically with students. The term includes classroom teachers, counselors, principals, librarians, paraprofessionals, nurses, educational diagnosticians, school psychologists, and athletic trainers.

An employee who communicates electronically with students shall observe the following:

- The employee is prohibited from knowingly communicating with students using any form of electronic communications, including mobile and web applications, that are not provided or accessible by the district unless a specific exception is noted below.
- Only a teacher, trainer, or other employee who has an extracurricular duty may use text messaging, and then only to communicate with students who participate in the extracurricular activity over which the employee has responsibility. An employee who communicates with a student using text messaging shall comply with the following protocol:
 - The employee shall include at least one of the student's parents or guardians as a recipient on each text message to the student so that the student and parent receive the same message;
 - The employee shall include his or her immediate supervisor as a recipient on each text message to the student so that the student and supervisor receive the same message; or
 - For each text message addressed to one or more students, the employee shall send a copy of the text message to the employee's district email address and respective supervisor.
- The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity). Employees should exercise caution, sound judgment, and common sense in respect to the appropriate times for communication.
- The employee is prohibited from knowingly communicating with students through a personal social network page; the employee must utilize a district-approved social network page for the purpose of communicating with students. The employee must enable administration to access the employee's page if electronically communicating with a student. Any page used to communicate with students must be approved by the Superintendent or designee.
- The employee does not have a right to privacy with respect to communication with students and parents and may be monitored at the district's discretion.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Texas Educators' Code of Ethics including:
 - Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records. (See *Policies CPC and FL*)
 - Copyright law. (See *Policy CY*)
 - Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student. (See *Policy DH*)
- Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with one or more currently-enrolled students.
- Upon written request from a parent or student, the employee shall discontinue communicating with the student through email, text messaging, instant messaging, or any other form of one-to-one communication.
- All staff are required to use school email accounts for all electronic communications with parents. Communication about school issues through personal email accounts or text messages are not allowed as they cannot be preserved in accordance with the district's record retention policy.
- An employee shall notify his or supervisor in writing within one business day if a student engages in an improper electronic communication with the employee. The employee should describe the form and content of the electronic communication.

Public Information on Private Devices

(Policies DH, GB)

Employees should not maintain district information on privately owned devices. Any district information must be forwarded or transferred to the district to be preserved. The district will take reasonable efforts to obtain public information in compliance with the Public Information Act. Reasonable efforts may include:

- Verbal or written directive
- Remote access to district-owned devices and service