Texarkana
Independent School District
The Place To Be!

TECHNOLOGY ACCEPTABLE USE POLICY

INFORMATION TECHNOLOGY DEPARTMENT
410 Westlawn Drive • Texarkana, Texas 75503
www.txkisd.net

PRINCIPAL OFFICIALS & ADVISORS

BOARD OF TRUSTEES

Fred Norton, Jr., President
Gerald Brooks, Vice President
Amy Bowers, Secretary Wanda Boyette
Bryan DePriest
Bill Kimbro
Paul Miller

A DMINISTRATION

Autumn Thomas, Acting Superintendent
Holly Tucker, Chief Academic Officer
Rusty Ogburn, Director of Information Technology

ACCEPTABLE USE POLICY COMMITTEE

Holly Tucker, Chief Academic Officer
Rusty Ogburn, Director of Information Technology
Chris Davis, IT Senior Systems Administrator
Phillip Watson, IT Senior Systems Administrator
Christy Tidwell, Executive Director of Curriculum and Instruction
Cathy Klopper, Director of STEM
Jennifer Beck, Coordinator of Secondary Instructional Technology
Kim Icenhower, Coordinator of Elementary Instructional Technology

T ABLE OF CONTENTS

PURPOSE

The technology resources at Texarkana Independent School District support the educational, instructional, and administrative activities of the District. These technologies, when properly used, promote educational excellence in the District by facilitating collaboration, innovation, and communication with the support and supervision of parents, teachers, and support staff. The use of Texarkana ISD technology resources is a privilege, not a right, and should be treated as such.

Texarkana ISD believes that the value of providing information, interaction, and resource capabilities far outweigh the possibility that users may procure material that is not consistent with the educational goals of the District. Texarkana ISD complies with Federal regulations regarding Internet filtering in order to limit user access to inappropriate content. Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Texarkana ISD activities. This document is intended to clarify those expectations as they apply to computer and network usage and is consistent with District policy as well as guidelines at the local, state, and national levels. Any user who does not comply with policies and procedures may face appropriate disciplinary actions. Users should not have any expectation of privacy when using District technology resources.

SCOPE

This policy applies to anyone who uses Texarkana Independent School District technology resources. Technology resources include all District owned, licensed, or managed hardware and software as well as the use of the District network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

DEFINITIONS

The District's computer systems and networks include but are not limited to the following:

- ➔ Computer hardware and peripherals
- ➔ Servers
- ➔ Email
- ➔ Databases
- ➔ Software including operating system software and application software
- ➔ Externally accessed data including the Internet
- ➔ Network Storage
- ➔ Digitized information including stored tests, data files, email, digital images, and video and audio files
- ➔ District provided Internet access
- ➔ District provided public Wi-Fi
- ➔ New technologies as they become available

POLICY

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 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).

Electronic Mail

Email is the primary form of communication in Texarkana ISD. The following guidelines must be understood and adopted in your daily operations.

Electronic mail is a privilege, not a right. User responsibilities and consequences for policy violations apply to email as well as other communication devices (i.e., desk phone, cell phone, two-way radio, etc.).

Public Information Act. The software and hardware that provides us email capabilities has been publicly funded. For that reason, it should not be considered a private, personal form of communication. The contents of any email communications are governed by this Acceptable Use Policy and subject to the Public Information Act. The District must comply with any legal requests for access to email contents.

No Blanket emails. District-wide emails must have prior authorization from a department Chief or designee. The District has established distribution lists to ensure emails are sent only to intended personnel. Select "group" recipients appropriately. The District email system should not be used for mass mailings except when approved by a Chief and for official District business.

Misaddressed emails. Incoming email that is misaddressed will remain "undeliverable". It is your responsibility to ensure you give out your correct email address.

Requests for Information. Independent verification is required before responding to requests for personal information on students or staff members. All information requests should be directed to the District's Public Information Officer.

Release of Student Records. No request for student grades, discipline, attendance or related information can be communicated via email unless a signed Release of Student Records is on file on the campus.

Personal emails. Personal email should not impede the conduct of District business; only incidental amounts of employee time (time periods comparable to reasonable coffee breaks during the day) should be used to attend to personal matters. Employee time may be restricted by a supervisor or campus administrator. **District E-Mail accounts should NEVER be used for personal email. District accounts can be used for subscriptions to websites or blogs a s long as they are for educational purposes only.**

Chain Letters. Since email access is provided for District related use, please do not forward messages that have no educational or professional value. An example would be any number of messages that show a cute text pattern or follow a "chain letter" concept. These messages should be deleted.

Attachments to email messages should include only data files. At no time should program files (typically labeled ".exe") be attached due to software licensing requirements. In addition, there exists the real possibility that any program files received as attachments over the internet may include viruses or other very destructive capabilities once they're "launched" or started. In addition to .exe files, some common types of file extensions that might indicate a file is dangerous include .com, .pif, .bat, and .scr. If you receive an attachment like this, delete the email message immediately without saving or looking at the attachment. If you think you may have opened a suspicious attachment, report the incident to the Technology Department immediately.

Avoid phishing scams. Phishing email will typically direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has.

Listservs/Blogs. Subscriptions to an Internet listserv should be limited to information related to your profession.

Records Retention. Each employee shall comply with the District's requirements for records retention and destruction to the extent those requirements apply to electronic media. **(see Board Policy CPC Local)**

Automatic forwarding of emails to a third-party email system is prohibited. Individual messages which are forwarded must not contain Texarkana ISD confidential information.

No official business using third-party email. Users are prohibited from using third party email and storage servers to conduct Texarkana ISD business. Such communications and transactions should be conducted through proper channels using Texarkana ISD approved methods. Personal email accounts used to conduct District business may be subject to Public Information Requests.

No expectation of privacy. Users should have no expectation of privacy in anything they store, send, or receive on the District's email system. Messages may be monitored without prior notice.

Email addresses are assigned at the discretion of the Technology Department based on a user's legal name. In some circumstances, it may be necessary to change your email address. Technology can assign a new address at its discretion.

Local Computer Hard Drives and Data Storage

Some computers may allow access to the local hard drive for storing files. This access does not mean that personal software should be installed on District computers. Only pre-approved software should be installed and only by technology staff.

How and Where to store files:

Texarkana ISD directs all staff to use their District assigned Google Drive for storing all files. These Google Drives have unlimited storage and are fully protected against hardware failure and accidents. If Google Drive is unavailable files can be saved to My Documents (also known as the H: drive), the desktop of the local computer, or a USB flash drive. It is important to remember that anything saved locally to a computer or flash drive is not protected in the event of physical damage or against encryption by computer malware. Google Drive should be the primary storage location for your files, and other locations should be treated as secondary or temporary.

The Texarkana ISD IT Department also reserves the right to reimage District computers when upgrading or in cases of malware infection at a moment's notice. This would result in the complete loss of any files stored on a computer's local hard drive. You are personally responsible for making backups of any files that are stored on your local computer's hard drive.

Hardware Purchasing

The Technology Department must authorize all hardware purchases. The authorization process includes testing of hardware for compatibility and functionality.

- All hardware must be purchased through and shipped to the Technology Department with documentation listing campus name and contact. (Please review the **Texarkana ISD Approved Hardware List prior to placing an order.**)
- Campus computer systems may not be modified, upgraded, or replaced with donated equipment without the prior approval of the Director of Information Technology.
- To maintain accurate physical inventory desktop computer systems should not be moved from one campus to another without prior approval of the Technology Department.

Software Purchasing

Step 1: Classroom Instructional Software Approval - All requests for approval to purchase an instructional software must be reviewed by the TISD Instructional Technology Specialists
(jennifer.beck@txkisd.net and/or ***kim.icenhower@txkisd.net***)

Step 2: Software Approval for System Alignment - Once a software request has been approved by the Instructional Technology Specialists, the technology department must review to ensure that the required support and installation process aligns with the district network.

Our goal is to promote the use of appropriate and approved software whenever possible. These guidelines will ensure that the required support and installation process is in place before funds are expended.

To ensure that software will not affect the current network configuration adversely, the following guidelines apply when you want to purchase software.

- Initial approval must be obtained from the TISD Instructional Technology Specialists office at Instructional Services.
- All software purchases must be purchased through and delivered to the Technology Department for installation.
- Software will be installed only when there is documentation showing that the software purchase has gone through the process referenced above and that proper licensing has been purchased.
- Only Technology staff or an authorized vendor shall install computer software on District computers.
- If a software program is determined to be unsuitable for the network or current environment it should not be purchased.

Electronic Communication with Students, Staff, and Parents/Guardians

The following definitions apply for the use of electronic communication 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 e-mail, text messages, instant messages, and any communication made through an Internet website, including any social media website or any social networking website.

Communicate means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at a student (e.g., a posting on the employee's personal social network page or blog) is not a communication; however, the employee may be subject to District regulations on personal electronic communications. See Personal Internet Postings/ Social Media Sites above. Unsolicited contact from a student through electronic means is not a communication.

Certified or licensed employee 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, licensed therapists, and athletic trainers.

Participation in Social Media Sites

The Internet, along with next-generation communication tools, has expanded the way in which employees can communicate internally and externally. While this creates new opportunities for communication and collaboration, it also creates new responsibilities for District employees. Social media sites include all forms of social media, such as text messaging, instant messaging, electronic mail (email), web logs (blogs), electronic forums (chat rooms), video-sharing websites (e.g., YouTube), editorial comments posted on the Internet, and networking websites (e.g., Facebook, MySpace, Twitter, LinkedIn). Social media also includes all forms of telecommunication such as landlines, cell phones, and web-based applications. All of these activities are referred to as "Social Media Sites" in this Acceptable Use Policy. Employees are encouraged to maintain separation between personal and professional postings for Social Media Sites. Conduct on social media sites is governed by B oard Policy DH (Local).

Professional Internet Postings/Social Media Sites

Professional Internet Postings/Social Media Sites that are school-based should be designed to address reasonable instructional, educational, or extra-curricular program matters. Employees are required to obtain approval and guidance from the District's Public Relations department before setting up a professional social media presence. The District reserves the right to remove, disable, and provide feedback regarding professional social media sites that do not adhere to District policy or standards of operation. The following guidelines will apply for any employee who uses social media for professional purposes:

- Professional sites should include language identifying the sites as professional social media sites of the District or campus.
- Employees should exercise caution, sound judgment, and common sense when using professional social media sites. The District's Public Relation department will regularly monitor professional social media sites to protect the school community.
- When establishing professional social media sites, supervisors and employees should consider the intended audience for the site and consider the level of privacy assigned to the site, specifically, whether the site should be a private network or a public network.
- The employee is subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators when communicating regarding professional, work-related matters, regardless of whether the employee is using private or public equipment, on or off district/campus property. These restrictions include:

    - Confidentiality of student records [see Board Policy FL ***(Legal)***, ***(Local)***].
    - Confidentiality of health or personnel information concerning colleagues unless disclosure serves lawful professional purposes or is required by law (see Board P olicy DH Exhibit).
    - Confidentiality of District records, including educator evaluations and private email addresses ***(see Board Policy GBA).***
    - Copyright Laws [see Board Policy CY ***(Legal)***, ***(Local)***].
    - Prohibition against harming others by knowingly making false statements about a colleague or the District ***(see Board Policy DH Exhibit)***.

Personal Internet Postings/Social Media Sites

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 social media as they are for any other public conduct. If an employee's personal use of social media 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 media 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. The following guidelines will apply for any employee who uses social media for personal purposes:

- The employee's use of social media for personal purposes should impose no tangible cost on the District; should not unduly burden the District's technology resources; and should have no adverse effect on an employee's job performance or on a student's academic performance.
- If an internet posting makes it clear that the author works for the District, it should include a simple and visible disclaimer such as, "these are my personal views and not those of the District." When posting your point of view, you should neither claim nor imply you are speaking on the District's behalf.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators when communicating regarding professional, work-related matters, regardless of whether the employee is using private or public equipment, on or off district/campus property. These restrictions include:

    - Confidentiality of student records [see Board Policy FL ***(Legal)***, ***(Local)***].
    - Confidentiality of health or personnel information concerning colleagues unless disclosure serves lawful professional purposes or is required by law ***(see Board Policy DH Exhibit)***
    - Confidentiality of District records, including educator evaluations and private email addresses ***(see Board Policy GBA)***.
    - Copyright Laws [see Board Policy CY ***(Legal)***, ***(Local)***].
    - Prohibition against harming others by knowingly making false statements about a colleague or the District ***(see Board Policy DH Exhibit)***

- The employee should not "tag" photos of other District employees, volunteers, contractors, or vendors without the prior permission of the individuals being tagged.
- The employee shall not use the District's logo or other copyrighted material of the District without consent of the District's Public Relations department.
- Photos or videos of students should not be posted on an employee's personal Social Media pages.

Use of Electronic Media for Communication with Students and Parents/Guardians

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may communicate through electronic media with students and parents/guardians who are currently enrolled in the District about matters within the scope of the employee's professional responsibilities. The employee is prohibited from knowingly communicating with students and parents/guardians using any form of electronic communications, including mobile and web applications, that are not provided or accessible by the District without supervisor approval. Currently, the District recommended list of electronic communications include:

- TEAMS
- GMail
- Google Meet
- Google Chat
- Google Classroom
- Remind

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

➔ Text messaging from employee cell phones to students is prohibited unless school-related and approved by their supervisor. A teacher, trainer, or other employees who has an extracurricular duty may use text messaging, with approval from their supervisor. Any text messaging for instructional purposes such as classroom student response systems must be approved by the supervisor prior to use in the classroom. With special approval from their supervisor, a teacher or other employee may use text messaging and then only to communicate with students over which the employee has responsibility regarding school-related information. 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; or
- 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 designated 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 classwork, 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 communications with students and parents and maybe 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 Educator's 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 Board Policies CPC ***(Legal)***, ***(Local)*** and FL ***(Legal)***, ***(Local)***].
- Copyright law [see Policy CY ***(Legal)***, ***(Local)***].
- Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student. [see Policy DH ***(Legal)***, ***(Local)***, ***(Exhibit)***].

➔ 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 employees shall discontinue communicating with the student through email, text messaging, instant messaging, or any other form of one-to-one communication.

➔ All staff is 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/her supervisor, in writing, within one business day if a student engages in improper electronic communication with the employee. The employee should describe the form and content of the electronic communication.

All other employees (outside the scope of professional responsibilities) are prohibited from communicating with students who are enrolled in the District through social media sites. An employee is not subject to these provisions regarding electronic communications with a student to the extent the employee has a family or existing social 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 acknowledgment 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 exempt from District regulation; and
- The parent is solely responsible for monitoring electronic communications between the employee and the student.

Inappropriate Communication with Students

Employees shall refrain from inappropriate communication with a student or minor, including but not limited to, electronic communication such as cell phone, text messaging, email, instant messaging, blogging, or other social media communication. Factors that may be considered in assessing whether the communication is inappropriate to include, but are not limited to:

- The nature, purpose, timing, and amount of communication;
- The subject matter of the communication;
- Whether the communication was made openly or the educator attempted to conceal the communication;
- Whether the communication could be reasonably interpreted as soliciting sexual contact or a romantic relationship;
- Whether the communication was sexually explicit; and
- Whether the communication involved discussion(s) of the physical or sexual attractiveness or the sexual history, activities, preferences, or fantasies of either the educator or the student.

EXCEPTIONS

Any requests for exceptions to this policy must be submitted in writing and will be reviewed on a case by case basis. Exceptions shall be permitted only after written approval from the Director of Information Technology or responsible Information Technology designee. The list of exceptions shall be reviewed annually and canceled as required.

SANCTIONS

Known violations of the policy will be addressed by disciplinary policies and procedures applicable to the individual.

All known and/or suspected violations must be reported to the applicable department head, who will report, as appropriate, to the applicable department. All such allegations of misuse will be investigated by the appropriate District administrative office with the assistance of Information Technology and the Office of Human Resources.

Penalties may include:

- Suspension or termination of access to a computer and/or network resources;
- Suspension or termination of employment, to the extent authorized by other Texarkana ISD published policies and procedures;

- Suspension or termination of contract, computer, and/or network services; or
- Prosecution to the full extent of the law.

DISCLAIMER

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected. Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's Technology Resources.

The District will, at its own discretion, monitor any technology resource activity without further notice to the end-user.

Headings are for convenience of reference only and shall not be used in the interpretation of this document.

TERM

This policy is binding for the duration of an employee's employment with the Texarkana Independent School District and must be reviewed and signed annually at the start of each school year.