STUDENT TECHNOLOGY ACCEPTABLE USE POLICY

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 your assignments, academic work and web-based platforms. Make sure not to store any passwords in easily accessed locations.
- 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.

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. Within two weeks of initial enrollment and subsequently at the beginning of the school year, the parent/guardian of the student must sign and return the appropriate TISD Student Technology Acceptable Use form in order for the student to retain internet access. If internet access is removed from the student's login for this reason, it will be reinstated upon receipt of the Student Handbook form.

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.

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

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 educational process; only incidental amounts of time should be used to attend to personal matters. Student time may be restricted by a staff member 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. In addition, there exists the real possibility that any files attached to emails may contain viruses or other malware. Be on guard when you receive emails with attachments without any prior discussion or warning from strangers or even people you know. 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.

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

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.

How and Where to store files:

Google Drive should be the primary storage location for your files. Many elective classes require an alternative storage location for your class files. Your teacher will instruct you on how to access and use that storage location.

Electronic Communication with Students, Staff, and Parents/Guardians

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. Unsolicited contact from a student through electronic means is not a communication.

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

Inappropriate Communication with Teachers

Students shall refrain from inappropriate communication with an employee, 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 student 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.

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;
- Discipline in accordance with the Student Code of Conduct, and, in some cases, the consequences may rise to the level of expulsion.

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.*