TOMBALL

INDEPENDENT SCHOOL DISTRICT

Digital Resources Acceptable Use and Internet Safety Policy

2024-2025

TISD Digital Resources: Acceptable Use and Internet Safety Policy

Access to TISD's technology resources will be through a District authorized account. Tomball ISD provides users access to district resources, including, but not limited to: devices, networks, G Suite for Education including YouTube, Web applications and other Internet services for **educational purposes only**.

A user, when utilized within this document, is defined as:

- Tomball ISD Employee or Board Member
- Tomball ISD Students
- Student Teacher
- Temporary Worker (Substitute Teachers, Consultants, etc.)
- Any third party that uses technology resources in Tomball ISD

Terms and Conditions

While digital resources offer tremendous educational opportunities, it is important to remember that access is a privilege, not a right, and carries with it responsibilities for all involved. The district wants all users to be aware of conduct considered acceptable and unacceptable.

- All District digital resources may be monitored whether the use is directly related to school or related to personal business.
    - Monitoring will take place upon the request from the TISD Superintendent or designee.
    - The information gathered from the monitoring procedures may be used to provide information regarding appropriate or inappropriate use of the District digital systems and/or required by an authorized legal authority.
- There is no guarantee of privacy, even for "personal" messages.
- Any user identified as a security risk or having violated District and/or campus technology use guidelines may be denied access to any TISD digital resource.
- At the beginning of each school year, all users are responsible for reading and adhering to the Acceptable Use and Internet Safety Policy.
- Computer programs, websites, and applications that have not been purchased by the district must be reviewed per the TISD vetting process prior to use by students.
- All users must adhere to the copyright laws of the United States (P.L. 94-553) and the Congressional guidelines that address software, authorship, and copying information.
- All acceptable use guidelines apply to both district digital resources and personal devices.

Safe Use of Technology

The district is committed to ensuring that students use technology safely and will follow all federal and state requirements to protect students from excessive data collection or materials that are considered harmful to minors. The district considers parents as partners in cybersecurity and online safety.

In accordance with state and federal law, the district will:

- Install a filter that blocks and prohibits pornographic or obscene materials or applications, including from unsolicited pop-ups, installations, and downloads, before transferring an electronic device to a student to be used for an educational purpose
- Block or filter students' internet access to pictures that are obscene, contain child pornography, or have been determined to be harmful to minors in accordance with the Children's Internet Protection Act (CIPA)
- Require direct and informed parental consent for a student's use of software, other than software excluded from the consent requirement by law
- Require direct and informed parental consent for a student's use of software that conducts mental health assessments or other assessments unrelated to education curricula that are intended to collect information about students

If you want to know more about partnering with the district regarding cybersecurity and online safety, or if you have complaints or concern about student use of electronic devices, please contact the Director of Technology Services at 281-357-3052.

District Network Filtering

Users with access to the Internet through TISD's Network (wired or wireless) will be filtered and blocked from visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by CIPA and as determined by the Superintendent or designee. However, because of the efficiency and ease of creating websites and the increased knowledge and awareness of available methods to bypass Internet filtering systems, it is extremely difficult to completely block every site with objectionable material. The TISD Technology Department, in conjunction with district administrators, campuses, and teachers, continually update the filtering system in an effort to block, to the greatest degree possible, objectionable websites and questionable material.

A user who gains access to objectionable or inaccurate material is expected to discontinue the access as quickly as possible and to report the incident to the appropriate supervisor (teacher, administrator, or district personnel). The site address will be added to filtering software, so that it can be removed from accessibility.

Personal Devices

Personal digital devices are defined as privately owned wireless devices and/or portable electronic hand-held equipment that include, but are not limited to, laptops and mobile computers, smart phones, tablets, e-readers, and portable internet devices. Students must obtain prior approval before using personal digital devices in the classroom. All the conditions and requirements of the TISD Acceptable Use Policy are applicable to the use of personal digital devices and violations may result in loss of privileges and/or disciplinary action.

- Personal digital devices will be used exclusively for educational activities during instructional class periods with express permission from the teacher.
- While at school, students will use the district's secured, CIPA compliant (filtered) public wireless network. Connecting a personal digital device to the district's wired network is not allowed.
- No student shall establish a wireless ad-hoc or peer-to-peer network using his/her personal device while at school. This includes, but is not limited to using a privately owned device as a cabled or wireless hotspot.
- Students may not use their personal technology devices to record, transmit or post photos or videos at school without the express permission of the teacher or campus administrator.
- Students will not loan their device to someone else. The user is responsible for the content contained on the device regardless of how it originated and is responsible for the security of any equipment brought with them to school.
- TISD is not responsible for, nor will TISD reimburse employees or students for any data and/or SMS/MMS (texting) charges.
- TISD **is not** responsible for any financial expenses or loss of data should a personal technology device be lost, stolen or damaged while at school.

Digital Citizenship Instruction

Each year instruction will be provided to all users regarding appropriate online behavior, including cyber-bullying awareness and response, as well as interacting appropriately with other individuals on the Internet. All users will be provided copies of the District's Acceptable Use and Internet Safety Policy.

It shall be the responsibility of all members of the Tomball ISD staff to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with the Children's Internet Protection Act and the Children's Online Privacy and Protection Act (COPPA).

Online Harassment Law

Users shall not harass others with language, images, or threats.

1. An offense under Penal Code Title 7 Chapter 33 Subsection (a) is a felony of the third degree. An offense under Penal Code Title 7 Chapter 33 Subsection (b) is a Class A misdemeanor, except that the offense is a felony of the third degree if the actor commits the offense with the intent to solicit a response by emergency personnel.
2. A person commits an offense if the person uses the name or persona of another person to create a web page or to post one or more messages on a commercial social networking site:
    a. without obtaining the other person's consent; and
    b. with the intent to harm, defraud, intimidate, or threaten any person.
3. A person commits an offense if the person sends an electronic communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:
    a. without obtaining the other person's consent;
    b. with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and/or
    c. with the intent to harm or defraud any person.
4. If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

Unacceptable Use of Devices, Networks, and District Accounts

1. Any malicious attempt to harm or destroy Tomball ISD digital resources, data of another user of the Tomball ISD system, or any of the agencies or other networks that are connected to the Internet is prohibited.
2. A deliberate attempt to hinder or disrupt the system performance may be viewed as a violation of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.
3. Users shall not use a computer for unlawful purposes, such as the illegal copying or installation of software. Only designated personnel may install software to any TISD digital resource.
4. Users shall not tamper with computers, networks, printers or other associated equipment except as directed by the Technology Department staff.
5. Users shall not move technology equipment (hardware or software) to any other location without written permission from the Director of Technology Services.
6. Users shall not deliberately access or create any obscene or objectionable information, language, or images.
7. Users shall not erase, rename, or make unusable anyone else's computer files, programs or storage devices..
8. Users shall not use, share their own nor attempt to access another user’s name, log-on, password, or files for any reason (except authorized staff members).
9. Users shall not use any social media learning environments unless they are within a District-approved, safe, secure, curriculum-supported learning activity.
10. Users shall not use any non-school sponsored chat rooms or instant messaging services.
11. Users shall not attempt to circumvent the content filtering system through unauthorized means (e.g. proxies, hacking, etc.).
12. Users shall not stream media from services such as YouTube, Internet Radio or other online media services for any purpose other than educational and shall not attempt to circumvent the Content Filter.
13. Users shall not utilize personal accounts to stream media from sources such as; Netflix, Disney+, etc. (US Copyright 17 US Code §110)
14. In accordance with state law, the district prohibits the installation or use of Tik Tok (or any successor application or service) on a district device, along with any other social media application or service determined by the governor.

The Use of Artificial Intelligence by Students

"Artificial Intelligence" ("AI") refers to systems or machines that mimic human intelligence to perform tasks and can improve their performance based on experience. This includes but is not limited to, AI-powered software, applications, tools or platforms, machine learning, and natural language processing technologies.

Students must do their own work and use their own cognitive abilities to complete assignments, exams, research, and other evaluated school work. The use of AI to shortcut or replace this process is considered a violation of academic integrity. All work submitted for academic credit must be the original work of the student.

Electronic Communication and Sharing

Electronic Communication and Sharing is the process of sending or sharing information or files through electronic means like email or file sharing in G Suite for Edu. Users are obligated to use these methods of communication in a responsible, effective and lawful manner taking into consideration the nature of the material being sent or shared. Therefore, it is important to note that users and/or the District may be held legally liable for:

- sending or sharing electronic communication with any libelous, defamatory, offensive, racist or obscene remarks;
- forwarding or sharing electronic communication with any libelous, defamatory, offensive, racist or obscene remarks;
- unlawfully forwarding, sharing or copying confidential information without permission; and/or
- sending or sharing information that contains a virus.

Unacceptable Use of Electronic Sharing and Communication

Any communication by electronic means may not be used to:

- send district-wide communication without proper authorization
- electronic communication sent by users may not contain abusive or threatening language, support cyber bullying, must not be sent anonymously or under a false identity and/or contain expressions of bigotry or hate, profanity, obscene comments, inappropriate materials, political lobbying or product advertisement
- transmit commercial software. This includes sending any copyrighted materials belonging to parties outside of the district itself
- create and/or send "spam." Spam is defined as any unsolicited electronic communication that is sent to any number of recipients who did not specifically request or express an interest in the material advertised in the communication. Unsolicited commercial Email or “Spam” is not permitted by state law
- practice an activity designed to deny the availability of electronic communications resources. Also called "denial of service attacks," these activities deny or limit services through mail bombing, malicious executables such as viruses, threatening a virus, or opening a large number of mail connections to a mail host or SMTP relay
- conduct any communication or include any links intended for personal financial gain;
- conduct any communication that violates other District policies or guidelines;

Consequences of an AUP Violation

Violation(s) as defined above will result in:

- suspension of access to the digital resources;
- revocation of the computer system account;
- restitution for costs associated with system restoration of hardware or software; or
- other disciplinary or legal action in accordance with the District policies and applicable laws.

Disclaimer of Liability

The District shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions or other laws, users' mistakes or negligence, or costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

The Tomball ISD system is provided on an "as is, as available" basis. Tomball ISD does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services, information or software provided.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third party individuals are those of the providers and not the District.

Tomball ISD will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the Tomball ISD electronic communication system.

If any user disregards the rules set out in TISD’s Acceptable Use Policy, the user will be fully liable and Tomball ISD will disassociate itself from the user as far as legally possible.