



Tomball Independent School District

**Technology Resources
Acceptable Use and
Internet Safety Policy**

2014-2015

TISD Technology Resources Acceptable Use and Internet Safety Policy

Tomball ISD provides users access to technology resources, including, but not limited to: computers, networks, Google Apps for Education, Skype, Web 2.0 applications and other Internet services for **educational purposes only**.

A user (actor) 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 vendor that uses technology resources in Tomball ISD

Terms and Conditions:

While electronic information 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. Access to Tomball ISD's technology resources will be governed as follows:

- With the approval of the immediate supervisor, District users will be granted access to TISD's technology resources.
- Any system user identified as a security risk or having violated District and/or campus technology use guidelines may be denied access to any TISD technology resource.
- At the beginning of each school year, all users are responsible for reading and accepting the Acceptable Use Policy.
- 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 policies apply to both district technology resources and personal devices.

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 guidelines.

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, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Monitoring of all District Provided Systems:

- All District technology resources may be monitored whether the use is directly related to school or 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 computer systems and/or required by an authorized legal authority.
- There is no guarantee of privacy, even for "personal" messages.

Internet/Intranet Guidelines, Safety/Filtering, & Social Networks:

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.

- Access to TISD's technology resources will be through a District authorized account and for **educational purposes only**.

- Users shall not erase, rename, or make unusable anyone else's computer files, programs or disks.
- 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 Technology staff members).
- Users shall not use personal devices or TISD computers/networks for any non-instructional or non-administrative purpose (e.g. games or activities for personal profit).
- Users shall not deliberately access or create any obscene or objectionable information, language, or images.
- Users shall not use any social media learning environments (including but not limited to Facebook, blogs, discussion forums, RSS feeds, wikis, and message boards) unless they are within a District-approved, safe, secure, curriculum-supported learning activity.
- Users shall not use any non-school sponsored chat rooms or instant messaging services.
- Users shall not attempt to circumvent the content filtering system through unauthorized means (e.g. proxies, hacking, etc.).
- Streaming media; such as YouTube, Internet Radio, and other online media are for **educational purposes only** and any attempt to circumvent the Content Filter is prohibited.

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

In some cases, students may find it beneficial or might be encouraged to use personal technology devices while at school. Personal technology 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 technology devices in the classroom. All the conditions and requirements of the TISD Acceptable Use Policy are applicable to the use of personal technology devices and violations may result in loss of privileges and/or disciplinary action.

- Personal technology 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 technology device to the district's wired network is not allowed. Students should not use 3G/4G wireless service on campus.
- 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 video of a person or persons on the campus.
- Photos or video recorded at school are not to be transmitted or posted at any time without express permission from the 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 personnel will not provide technical service or support for, nor will they install any software on personal technology devices.
- 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

Acceptable Use

The District's technology resources must be used for **educational purposes only** and be consistent with the mission and goals of the Tomball Independent School District.

Unacceptable Use

Transmission of any material in violation of any US or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret. Use

for commercial activities is strictly prohibited. Use for product advertisement or political lobbying is also prohibited.

1. Any malicious attempt to harm or destroy Tomball ISD technology 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 without permission from the holder of the copyright and from the Director of Instructional Technology. Only designated personnel may install software to any TISD technology resource.
4. Users shall not copy, change or transfer any software or documentation provided by TISD, teachers, or a student without permission from the Director of Technology Services.
5. Users shall not tamper with computers, networks, printers or other associated equipment except as directed by the Technology Department staff.
6. Users shall not connect any personal devices to the TISD wired network. No personal networking equipment, such as Access Points, are permitted on the TISD network.
7. Users shall not move technology equipment (hardware or software) to any other location without written permission from the Director of Technology Services.
8. Users shall not access websites of non-instructional nature, including, but not limited to game sites (downloading or playing), websites containing objectionable material or images, and anonymous proxy sites.
9. Messages 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, or inappropriate materials.

Online Harassment:

Users shall not annoy or 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.

Email Conditions of Use

Email is a communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although email, by its nature, is less formal than other written communication, the same laws apply. Therefore, it is important to note that users and/or the District may be held legally liable for:

- sending emails with any libelous, defamatory, offensive, racist or obscene remarks;
- forwarding emails with any libelous, defamatory, offensive, racist or obscene remarks;
- unlawfully forwarding confidential information;
- unlawfully forwarding or copying messages without permission; and/or
- sending an attachment that contains a virus.

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.

Unacceptable Use of Email Services

District electronic mail services may not be used to:

- perpetuate chain email letters or their equivalents. This includes letters that require the recipient to forward an email to a specified number of addresses in order to achieve some monetary, philosophical, political, superstitious, or other goal. Emails that are part of a multilevel marketing or pyramid-selling scheme, sometimes known as "Ponzi schemes," are illegal in many places and are specifically forbidden under these standards;
- send district-wide communication without proper authorization from the Superintendent, Assistant Superintendent, or Director of Technology Services;
- 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;
- send or encourage "letter bombs." Letter bombs are extremely large or numerous email messages that are intended to annoy, interfere, or deny email use by one or more recipients;
- 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 without authorization or permission.,
- conduct unlawful activities. This includes any commercial purposes not under the auspices of the District;
- conduct any communication or include any links intended for personal financial gain;
- forward any email received in district to be automatically forwarded to an external destination;
- send or receive email attachments larger than 10 MB;
- conduct any communication that violates other District policies or guidelines;
- send abusive or threatening language;
- support cyber bullying;
- be sent anonymously or under a false identity; or
- contain expressions of bigotry or hate, profanity, obscene comments, or inappropriate materials.

Consequences of AUP Violation

Violation(s) as defined above will result in:

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

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 provided, or any information provided, or any software contained on the computer system; the system will meet the 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.

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.

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 for 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.