

Fort Stockton Independent School District
Technology Acceptable Use Policy Agreement
For FSISD Staff
Revised June, 2007

Please read this document carefully before signing.

Your signature on this document is legally binding and indicates the party who signed has read the (1) terms and conditions carefully, (2) understands the significance of this agreement, (3) and agrees to abide by all guidelines outlined in this agreement.

<h2>Employee AUP</h2>

Fort Stockton ISD Technology

A variety of technology, including but not limited to computers, software, and Internet Access are available to students of Fort Stockton Independent School District (hereafter referred to as "the District") through local and wide area network services. We are very pleased to bring this access to Fort Stockton Schools and believe these services offer vast, diverse, and unique resources to our employees and students. Our goal in providing these services is to promote educational excellence in schools for students and to facilitate employees of the district in their effort to provide efficient and economical quality education.

The smooth operation of our systems relies upon the proper conduct of all its users. It is very important that both you and your parents read and fully understand and abide by all aspects of the Fort Stockton ISD Student Acceptable Use Policy. Fort Stockton ISD owns all parts of the District's local (LAN) and wide area networks (WAN) and reserves the right to protect the integrity of the district local and wide area networks.

The FSISD Acceptable Use Policy complies with district Board Policy CQ Local and Legal, Electronic Communication and Data Management:

[http://www.tasb.org/policy/pol/private/186902/pol.cfm?DisplayPage=CQ\(LOCAL\).pdf](http://www.tasb.org/policy/pol/private/186902/pol.cfm?DisplayPage=CQ(LOCAL).pdf)
[http://www.tasb.org/policy/pol/private/186902/pol.cfm?DisplayPage=CQ\(LEGAL\).pdf&QueryText=COMPUTER%20POLICIES](http://www.tasb.org/policy/pol/private/186902/pol.cfm?DisplayPage=CQ(LEGAL).pdf&QueryText=COMPUTER%20POLICIES)

and contributes elaboration and other specific details pertaining to acceptable use of district computers, laptops, tablets, PDA's, smart phones, and other electronic devices, whether on or off district networks; and finally including acceptable use of the Fort Stockton ISD WAN (Wide Area Network) and LAN's (Local Area Networks). Employees and students will be held responsible at all times for the proper use of their FSISD network account.

Internet/Technology Safety Policy - The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. Fort Stockton ISD has taken measures to block and/or filter access to undesirable and inappropriate sites to maintain compliance with the Child Internet Protection Act (CIPA). An undesirable and inappropriate site is hereinafter defined as "one that portrays or depicts violence, profanity, partial and/or full nudity, sexual acts or text, gross depictions or text, intolerance, cult, drugs and drug culture, militant or extremist, gambling, and/or alcohol related content". While these protection measures are in place, it is impossible to filter all undesirable and inappropriate sites at all times. New sites are placed on the World Wide Web daily. As a result, students and adults may inadvertently or purposely connect to an undesirable and inappropriate site. Should a student or an employee of the district inadvertently access such a site, they should notify the Campus Principal, Campus Technology Contact, if applicable or Technology Coordinator immediately. As soon as the district is aware of any such site, measures will be taken to filter that site immediately.

While it is the district's intent to make Internet access available to further educational goals and objectives, individuals may find ways to access other materials as well. Fort Stockton ISD Technology may monitor online activities of students and employees without prior consent. Employees purposely visiting undesirable/inappropriate sites may be disciplined as outlined in section Consequences of *Improper Use – Employees*. Fort Stockton ISD firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the District.

Technology Use Terms and Conditions

The smooth operation of the District's local and wide area networks relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general this requires efficient, ethical and legal utilization of the network resources. An employee in violation of any of these provisions is subject to disciplinary action as stated in section Consequences of Improper Use – Employees.

1. **Permitted Use and Terms** - The use of the District's network and all technology services and resources is a privilege, not a right, and extends throughout an employee's term of employment, providing the employee does not violate the District's policies contained in this Acceptable Use Policy. Employees and students not in compliance with all parts of this Acceptable Use Agreement are subject to disciplinary actions outlined in section Consequences of Improper Use – Employees and Consequences of Improper Use – Students, respectively. Fort Stockton ISD administrative staff will determine what *improper use* is and their decision is final. The Administration may limit or revoke an account at any time as required without prior notification to the individual. The Administration of Fort Stockton ISD may request the Technology Coordinator to deny, revoke, or suspend or limit specific user accounts. The Technology Coordinator may deny, revoke, or suspend or limit user accounts that are deemed detrimental to the integrity of the network computing environment.
2. **Acceptable Use of the Internet** – The purpose of the Internet is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. The use of each employee account must be in support of education and research and consistent with the educational objectives of Fort Stockton ISD. Use of the District's technology network or resources for commercial activities, product advertisement or political lobbying, is strictly prohibited. Employees are expressly forbidden from accessing undesirable and inappropriate web sites, including gaming. Fort Stockton ISD networks and Internet services are NOT private. Use of any other organization's network or computing resources must comply with the rules appropriate for that network. This includes, but is not limited to the following: copyrighted material, threatening or obscene material, or material protected by trade secret. Use of commercial activities is not acceptable. Use for product advertisement or political lobbying is also prohibited. Employees are expressly forbidden from accessing undesirable and inappropriate sites (pornography, violence/profanity, partial nudity and art, full nudity, sexual acts/text, gross depictions/text, etc.) unless required to facilitate blocking and/or filtering of such sites.
3. **Email/Network Etiquette** - Email accounts are provided for employee educational use. Employees are encouraged to limit personal use of this account. Students of Fort Stockton ISD are not provided with Email accounts at this time. Employees are expected to abide by the generally accepted rules of email and network etiquette. These include, but are not limited, to the following:

- a. Employees are expected to check and respond to their FSISD email at least once a day.
- b. Employees are expected to return email communications to staff, parents, or other public members who have a legitimate educational request by the end of the next business day, whenever possible.
- c. Use only FSISD email accounts for district business. Most web-based email such as Yahoo, Hotmail, and Gmail are blocked by the filter. Only a few other web-based accounts (colleges, educational accounts, etc) are allowed within district networks.
- d. Delete old and unneeded email at weekly intervals to free valuable space on the file server.
- e. Use appropriate language. Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory or abusive language are prohibited.
- f. Employees will refrain from sending and/or forwarding items such as jokes, stories, etc. that have no educational or professional value. These items take up valuable server space and resources. When an item of this kind is received, delete it and do not send it to anyone else.
- g. Do not use the network in such a way that would disrupt the use of the network by other users.
- h. Illegal activities are strictly forbidden. Messages relating to or in support of illegal activities may be reported to the authorities.

- i. Generally, do not reveal personal information such as address or phone numbers or those of students or colleagues.
 - j. Electronic email is not private. The system administrator has access to all email. Your email may be monitored randomly to ensure proper use of email services and to systematically "clean out" old and/or unusually large mail taking up space on the server.
 - k. FSISD archives all email coming in and going out of the district, as required by the federal government (Dec. 2006). Communication mediums such as email, instant messages (IM), and other digital communications produced by employees are recorded and archived for 5 years.
 - l. All communications and information accessible via the network are property of Fort Stockton ISD and are subject to public information requests.
4. Public Information Act - In order to be in compliance with the Public Information Act, each employee is solely responsible for backing up and/or documenting any electronic information that is subject to the Public Information Act.

5. **Acceptable Use of Fort Stockton ISD technology, including, but not limited to: hardware, software, technology devices, and local and wide area networks**

The purpose of all components of the Fort Stockton ISD network(s) is to provide technology tools for students and employees for educational/business office use. District networks are designed, configured and maintained strictly for EDUCATIONAL PURPOSES ONLY. Violators of any of the following guidelines will be subject to ***Consequences of Improper Use - Employees.***

Employees and students should strictly adhere to the following guidelines:

- a. ONLY Fort Stockton ISD technology equipment such as computers, laptops, tablet PCs, PDA'S, or Smart Phones are allowed to access FSISD networks. Only FSISD equipment will be prepared by software installations and configurations to safely join the FSISD Domain.
NO OTHER TECHNOLOGICAL DEVICE IS ALLOWED ON DISTRICT NETWORKS.
- b. Non-educational gaming and other non-educational uses of technology is prohibited.
- c. Employees and students are prohibited from downloading or bringing from home or any other source any software and installing that software onto the local hard drive of any computer or onto the file server hard drive.
- d. Employees and students are prohibited from altering the computer hardware or software in any way.
- e. Employees and students are prohibited from changing any configuration of any computer or technology device. Do not try to repair the hardware or software at any time. Only authorized personnel are allowed to install, configure, and maintain hardware and software.
- f. Employees and students are prohibited from moving any computer(s) or technology devices without permission from the Technology Coordinator and the campus principal.
- g. Employees and students are prohibited from taking home or removing from school buildings/property any computer, laptop, tablet pc or technology device without written permission from the District Technology Coordinator. Technology checkout forms can be found online.
- h. Employees and students are to save files in designated storage locations designated by District Technology Coordinator.
- i. Employees and students are to login to the network using their unique login id and password. Employees and students are to NEVER, under any circumstances, login using anyone else's ID and password. Employees and students are to never share their password with anyone, except their Campus Technology Contact, if applicable, or District Technology Coordinator and/or District Network Admins/Technicians. If you suspect that someone else knows your password, you should contact the Technology Coordinator immediately and request a password change.
- j. Employees and students will be held responsible for the contents of their file storage location on the file server or the hard drive. Employees and students should monitor the contents and delete unnecessary items often. Should you suspect tampering with your files or file storage location, you should notify the Campus Technology Contact Coordinator immediately.
- k. Employees are held responsible for the contents and condition of computers and technology equipment in their work area. Employees must keep an up-to-date inventory of all computers/technology in their classroom and/or lab at all times. Employees should notify the Campus Technology Contact or District Technology Coordinator immediately should they suspect tampering with their technology. Employees may be held financially responsible for equipment in their room that is damaged or missing due to their negligence.

13. **Vandalism** - Vandalism is defined as any attempt to harm or destroy data or equipment of another user, Internet, or any other connected agency or other networks that are connected to the FSISD Internet backbone or any attempt to modify, delete, or add to the present network. Employees are strictly prohibited from performing vandalism acts of any kind to the District's technology resources. This includes, but is not limited to, the uploading or creation of viruses and other malware. In the event that you suspect that your computer has a virus or other malware, the Campus Technology Contact, if applicable or Technology Coordinator immediately.
14. **Forgery Prohibited** - Forgery or attempted forgery of electronic messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.
15. **Termination/Revocation of System User Account** – The District may suspend or revoke a system user's access to the District's system upon violation of any part of this Acceptable Use Policy and/or administrative regulations regarding acceptable use.
16. **Consequences of Improper Use - Employees** – Improper or unethical use may result in disciplinary actions. Employee actions not in compliance with the Acceptable Use Policy could result in:
 - a. Restricted in part or whole or revoked access to technology services
 - b. Formal employee reprimand and documentation
 - c. Restitution for costs associated with system restoration, hardware, software, etc. costs
 - d. Suspended from duty
 - e. Employment termination
 - f. Criminal charges filed
17. **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 fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District uses a variety of vendor-supplied hardware and Software. Therefore, 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 user's requirements. Neither does the District warrant that the system will be uninterrupted or error-free, nor 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 necessarily 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 computer systems and network.

Employee AUP

I understand and will abide by the Fort Stockton ISD Technology Acceptable Use Policy. I further understand that any violation of the regulations in the Fort Stockton ISD Technology Acceptable Use Policy is unethical and may constitute disciplinary action as outlined in the Consequences of Improper use – Employees section. Please sign below.

Print Name of **Employee** _____

Campus or Building _____

Signature of **Employee** _____ Date _____

Employee AUP **Permission to Video/Photograph**

Permission to video/photograph: I give FSISD permission to use my video/photograph on such mediums including, but not limited to newsletters, school newspapers, documents, and/or the District web page

Mark one of the following boxes:

- Yes**, I give my permission to use my photograph or video
- No**, I do not give permission to use my photograph or video

Print Name of **Employee** _____

Campus or Building _____

Signature of **Employee** _____ Date _____

Employee AUP **Permission to Display Work**

Permission to display employee work: I give FSISD permission to display my lesson plans, lessons, labs, projects, pictures, and/or videos to use on such mediums including, but not limited to newsletters, school newspapers, documents, and/or the District web page.

Mark one of the following boxes:

- Yes**, I give my permission to use my photograph or video
- No**, I do not give permission to use my photograph or video

Print Name of **Employee** _____

Campus or Building _____

Signature of **Employee** _____ Date _____