Fort Stockton Independent School District
Technology Acceptable Use Policy Agreement
for FSISD Staff

Revised January, 2018

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 a condition carefully, (2) understands the significance of this agreement, (3) and agrees to abide by all guidelines outlined in this agreement.

EMPLOYEE AUP

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 you 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, 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 may inadvertently or purposely connect to an undesirable and inappropriate site. Should a student inadvertently access such a site, they should notify the principal, teacher, Campus Technology Contact or Technology Director 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, students may find ways to access other materials as well. Fort Stockton ISD may monitor online activities of students without prior consent. Students caught visiting undesirable and inappropriate sites may be disciplined as outlined in section *Consequences of Improper Use – Students (page 7)*. 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.

- In accordance to the Protecting Children in the 21st Century Act, Fort Stockton ISD will provide for the education of minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, to minimize the incidence of cyber predation/stalking of our students, whether in school or at home.

- "Cyber-bullying" is defined as bullying through the use of technology or any electronic communication by such things as electronic mail, internet communications, instant message, text message, social media or facsimile. Cyber-bullying includes, but is not limited to:

  - ✓ ***Flaming***- deliberate sending or posting of electronic messages to a person(s) either privately or publically.
  - ✓ ***Impersonation***- when a person pretends to be or poses as another person. Once the impersonator has access to the victim's information, considerable damage can occur.
  - ✓ ***Sending malicious code***- intentionally to damage of harm the victim's system or to spy on the victim
  - ✓ ***Sending images and videos***-is a growing concern. Photographs and videos taken using cell phones of other students in bathrooms, locker rooms, or other compromising situations are easily distributed electronically, and sometimes published on video sites such as *YouTube*.
  - ✓ ***Trickery***- when a person purposely tricks another person into divulging secrets, private information or embarrassing information, and publically discloses that information online.
  - ✓ ***Sexting***- sending, receiving, or forwarding sexually suggestive nude or nearly nude photos or sexually explicit or suggestive messages through text message or email, usually with the consent of all persons involved, however, once an image or message is digitized, it is very easy to forward to anyone, including unintended recipients.
  - ✓ ***VIOLENCE and CRIMINALITY*** - engaging in bullying that encourages a student to commit or attempt to commit suicide; (2) inciting violence against a student through group bullying; or (3) releasing or threatening to release intimate visual material of a minor or a student who is 18 years of age or older without the student's consent.

It is the responsibility of every employee of the school district to recognize acts of online predation, cyber-bullying and retaliation. Any student who believes that he or she has been the victim of online predation/stalking, cyber-bullying or retaliation should report it immediately to his or her teacher or principal or other school official so that measures can be taken to end the abuse. All forms of electronic harassment either during school hours or after school hours will not be tolerated by Fort Stockton ISD.

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 (Page 8).*

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 Director to deny, revoke, or suspend or limit specific user accounts. The Technology Director 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 (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. 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.

3. **Email/Network Etiquette-** Email accounts are provided for employee educational use. Employees are encouraged to limit personal use of this account. 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. 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. Next, report the sender to your principal.
g. Do not send large files such as pictures and videos via district email. Rather, use the network drive Z: or the Bragging folder to save such files and direct users via a plain text email where to access your photo on the Z Drive.
h. Do not use the network in such a way that would disrupt the use of the network by other users.
i. Illegal activities are strictly forbidden. Messages relating to or in support of illegal activities may be reported to the authorities.
j. Generally do not reveal personal information such as address or phone numbers or those of students or colleagues.
k. 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.
l. 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 several years.
m. 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 education/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. At this time, only Fort Stockton ISD technology equipment such as computers, laptops, tablet PC's, Chromebooks 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.
   b. Non-educational gaming and other non-educational uses of technology is prohibited.
   c. Employees and students are prohibited from downloading or bringing into the district, any non-district software and installing that software onto the local hard drive of any computer/laptop or FSISD cloud drives or network drives.
   d. 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 I.T. personnel are allowed to install, configure, and maintain hardware and software.

e. Employees and students are prohibited from moving any computer(s) or technology devices without permission from the Technology Director and the campus principal.
f. Employees and students are prohibited from taking home or removing from school buildings/property any computer, or other technology device (except your assigned laptop or Chromebook) without written permission from the District Technology Director and approved by the campus principal. Technology checkout forms can be found online.
g. Employees and students are to save files in designated storage locations designated by District Technology Director for security. Those locations are backed up nightly.
h. 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 District Technology Director and/or District Network Admins/Technicians. If you suspect that someone else knows your password, you should contact the Technology Director immediately and request a password change.
i. Employees and students will be held responsible for the contents of their file storage location on the 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 Technology Director immediately.
j. 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 Technology Director 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.
k. Mobile technology items (laptops, cameras, document cameras, projectors, etc.) are to be kept locked away when not in use.
l. Employees and students are prohibited from using any method whatsoever to gain access to Administrator privileges to the local or wide area network. Employees and students are prohibited from viewing, modifying, adding to, or deleting any part of the system files or rights to system files of the local or wide area network. Any attempt will be considered as malicious hacking and will be dealt with accordingly. Should a teacher suspect a student accessing prohibited system resources, they should contact the Campus Technology Contact, if applicable, or Technology Director immediately.

6. **Hardware / Software Maintenance** – Fort Stockton ISD uses many technology utilities in day-to-day management of all parts of the network. Some of these utilities, while providing the capability to remotely manage user's computers, also provide opportunity for surveillance of user technology activity. Users are thus notified that at any time their technology activity could be monitored.

7. **Telecommunication Services** - Telecommunication services are provided as a service to employees for educational purposes. Employees should limit personal use of district telephones so that others have opportunity to use the telephone to call parents and/or conduct school business. All personal

long distance calls must be made with a calling card only. Some calling cards may/may not work with the school telephone system.

8. **Network Security** - Security on any computer system is a high priority. Measures have been taken to prevent outside sources from "hacking" into Fort Stockton ISD local and wide area networks and/or participating in other unlawful online activities. "Hacking" is defined as any attempt by an unauthorized user to change, alter, or break into the Fort Stockton ISD network. However, the district recognizes that industrious users may acquire and use such knowledge to participate in prohibited or unlawful online activities. Employees and students attending Fort Stockton ISD are strictly prohibited from hacking into or attempting to hack into the district local or wide area network or any network. If you can identify a security problem, you must notify the Technology Director immediately. Do not demonstrate the problem to others.

9. **Network Accounts**- Employees will be assigned a unique staff account for accessing district resources. Employees may not log into student computers with their employee network accounts and allow students to access the network/Internet through their employee accounts. Employees may not share their account with anyone or leave the account open or unattended. Attempting to log on to a computer or E-mail system by using another employee's account is prohibited.

10. **Personal Information** - Fort Stockton ISD protects student and adult personal information. Fort Stockton ISD is not responsible for any student or employee information being placed on any other web site whether school related or non-school related (i.e. Booster Club web site, student produced web sites, etc.).

11. **Copyright** - All employees and students of Fort Stockton ISD will comply with all copyright laws at all times.

12. **Warranty -** Fort Stockton ISD makes no warranties of any kind, whether expressed or implied, for the service it is providing. Fort Stockton ISD will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by anything whether it is the fault of outside influences, human or mechanical, or inside influences human or mechanical including, but is not limited to:
    a. "Acts of God" (lightening, summer heat, power outages, hardware & software failures, etc.)
    b. Improper use or non-use of your assigned network folders (W: Drive- public staff share and/or your assigned digital V: Drive - private)
    c. **Public shares, such as the S: drives, the W: drive, or the Z Drive are NOT SECURE**. Use them for sharing purposes only. Always have a backup of shared files in your V Drive. Anomalies, both human and network related, such as, deletion, disappearance, movement of folders, saving over files, and other such mishaps will and do occur.
    d. Negligence of your errors or omissions
    e. Use of any information obtained via the Internet is at your own risk. Fort Stockton ISD specifically denies any responsibility for the accuracy or quality of information obtained through its services.

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 Director 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 Acceptable Use Policy Agreement

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_____