Fort Stockton Independent School District
Technology Acceptable Use Policy Agreement
for Students

Revised January, 2018

Please read this document carefully before signing.
If the student is under the age of 18, a parent or legal guardian must also read and sign this agreement. 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.

STUDENT 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 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:
https://pol.tasb.org/Policy/Download/995?filename=CQ(LOCAL).pdf
https://pol.tasb.org/Policy/Download/995?filename=CQ(LEGAL).pdf
and contributes elaboration and other specific details pertaining to acceptable use of district computers, laptops, tablets, PDA's, touch slates, 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*. 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 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 student, parent and 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. A student in violation of any of these provisions is subject to disciplinary action as stated in section *Consequences of Improper Use – Students.*

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 the time a student is enrolled in the District providing the student does not violate the District's policies contained in this Acceptable Use Policy. A student not in compliance with all parts of this Acceptable Use Agreement is subject to disciplinary actions outlined in section *Consequences of Improper Use – Students.* 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 student 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.

3. **Email** - At this time, students are not given email accounts through the District's email services. However, should a student need the use of email in the course of a class, the teacher will provide monitored email access through a safe online student email account, such as Gaggle.net. When using email for school, students are expected to follow accepted email etiquette as well as the guidelines below:

a. Use appropriate language. Swearing, vulgarity, ethnic or racial slurs and any other inflammatory or abusive language are prohibited.
b. Proliferation and forwarding of jokes, stories, etc. that have no education value is prohibited. These items take up valuable server space and resources and potentially spreading embedded malicious code. When you receive an item of this kind, delete it immediately and do not send it to anyone else.
c. Illegal activities are strictly forbidden. Messages relating to or in support of illegal activities may be reported to the authorities.
d. Generally, do not reveal your personal address or phone number or those of students or school employees to anyone through email.
e. Electronic email is not guaranteed to be private. The teacher, system administrator, and Technology Director has access to all student email. Email may be monitored randomly to ensure proper use of email accounts.
f. All communications and information accessible via the school network are property of Fort Stockton ISD and are subject to public information requests.

4. **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 technology and network(s) is to provide technology tools for educational use only. Students are expected to abide by the generally accepted rules of network etiquette.

Students should strictly adhere to the following guidelines:

a. Students must have a signed Student AUP on file in order to access the World Wide Web (Internet).
b. Students are prohibited from downloading or bringing into the district via their network folders or any removable storage device, any software and installing that software onto the local hard drive of any computer. Students are strictly forbidden to participate in any type of illegal activity while using the District's technology resources.

c. Students are prohibited from signing into chat rooms unless under the direct supervision of their teacher for educational purposes.
d. Students will not create, copy, or transmit material which infringes the copyright of another person or organization (For example, plagiarism of electronic material of any kind).
e. Students will not willingly and purposely bypass or attempt to bypass district content filtering system.
f. Students are prohibited from accessing, creating, or transmitting material which is defamatory or designed to cause annoyance, inconvenience or needless anxiety of others (For Example: cyber bullying, hate mail), even if such activities occurred outside of school (For Example: uploads to MySpace, Facebook, Blogs and other hosting sites or email, or any live IRC or bulletin postings of any kind).
g. Students are prohibited from altering the computer hardware or software in any way. This includes changing any configuration of any computer or technology device. Do not try to repair the hardware or software at any time, even if a teacher or principal says it is okay. Only authorized personnel are allowed to install, configure, and maintain hardware and software.
h. Students are prohibited from moving any computer(s) or technology devices without permission from the Campus Principal, Campus Technology Contact, if applicable, or Technology Coordinator. Acts of non-compliance of this nature will be considered theft and offenders will suffer consequences outlined in section Consequences of *Improper Use – Students*.
i. District-provided bandwidth is reserved for educational and school district business purposes only. Students will not engage in activities which waste district network resources. (For example, non- educational uses of technology such as gaming of any kind unless used for educational purposes and is teacher directed, accessing or downloading music, movies, and/or videos whether **streaming* or other, creating or forwarding non-educational activities using district-provided mediums such as email, district bandwidth, or any other type of district communication.) **Streaming video is currently being utilized for educational use within the district, but is reserved strictly for teacher-led educational purposes only.*
j. Students should not reveal his/her personal address or phone numbers or those of any other person while using the Internet.
k. Students are to save their data files in storage locations designated by the District Technology Director only. The district is not responsible for lost data due to incorrect storage.
l. Students will not trespass in another person's folders, work, or files.
m. Students are to login to the Internet and their digital storage network using only their own unique login ID and password. Students are NEVER, under any circumstances, login using anyone else's ID and password. Students are NEVER to share their password with anyone, except a teacher, if needed. If you suspect that someone else knows your password, you should contact your classroom teacher, Campus Technology Contact, if applicable, or Technology Director immediately and request a password change.
n. Students will be held responsible for the contents of their file storage location on the Network Attached Storage (NAS) or in special instances, a local hard drive. Students should monitor the contents and delete unnecessary items in their folders often. Should you suspect tampering with your files or file storage location, you should notify your classroom teacher, or the Campus Technology Contact, if applicable, or the Technology Director immediately. Technology support staff will attempt to recover lost or damaged files only if those files were saved to the student's assigned data storage.
o. Students are prohibited from using any method whatsoever to gain access to Administrator privileges to the local or wide area network. Only designated technology staff may access parts of a system with that designated access. Any attempt will be considered as malicious hacking and will be dealt with accordingly. Should an employee or student suspect or witness any other person accessing prohibited system resources, they should contact the Campus Technology Contact, if applicable or Technology Director immediately. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the District's technology resources.

p. Students will not waste district resources, and are prohibited from using the network in such a way that would disrupt the use of the network for other users by engaging in activities which cause or are liable to cause disruption of district networks or denial of service to other users on district networks. (For example, introducing or attempting to introduce a virus, worm, Trojan, or spyware onto district networks).

q. No students or other children are permitted to work on district computers unsupervised, at any time.

5. **Hardware / Software Maintenance** – Fort Stockton ISD uses many technology utilities in day-to-day management of all parts of district networks. Some of these utilities, while providing the capability to remotely manage/maintain user computers, also provide opportunity for surveillance of user computer activity. Users are thus notified that at any time their technology activity could be monitored. Any information derived from surveillance could be used against this user.

6. **Telecommunication Services** - Telecommunication services are provided as a service for educational purposes. Students are allowed limited access to telecommunication services and may make local telephone calls with permission from their teacher or office personnel. All personal long distance calls must be made with a calling card only. Some calling cards may or may not work with the school telephone system. A local or long distance personal telephone call should never extend more than 5 minutes.

7. **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. If you can identify a security problem, you must notify a school administrator or the Technology Director immediately. Do not demonstrate the problem to others.

8. **Network Accounts -** Secondary students (Middle School and High School) will be assigned an individual account for accessing district resources. Students 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's account is prohibited.

9. **Copyright** - All Students of Fort Stockton ISD will comply with all copyright laws at all times.

10. **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:

- "Acts of God" (lightening, summer heat, power outages, hardware & software failures, etc.)
- Improper use or non-use of your assigned network folders (S: Drive- public student share and/or your assigned digital folder- private)
- Public shares, such as the S: drive, are **NOT SECURE**. Use them at your own risk. Anomalies, both human and network related, such as, deletion, disappearance, movement of folders, saving over files, and other such mishaps will and do occur.
- Negligence of your errors or omissions
- 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.

11. **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. Students 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. In the event that you suspect that your computer has a virus, notify your classroom teacher, the Campus Technology Contact, if applicable or Technology Director immediately.

12. **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.

13. **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 District policy and/or administrative regulations regarding acceptable use.

Examples of Offenses

The following are examples of 1st, 2nd, and 3rd degree offenses. This list is not all inclusive.

1st Degree Offenses
- Accessing the Internet without requesting permission from an instructor at each instance.
- Using chat or other communication software.
- Changing system or network settings (i.e. screen saver, backgrounds).
- Access storage devices without prior permission from the instructor.

2nd Degree Offenses
- Using obscene language.
- Downloading, installing, or attempting to install software or files (i.e. installing games, streaming music or video).
- Accessing or attempting to gain access to another user's password or account.
- Giving a password or account to another user.
- Violating copyright laws (i.e. plagiarism).

3rd Degree Offenses
- Harassing, threatening, or attacking others through the use of the network (cyber bullying).
- Damaging computers, computer systems or other computer networks including attempting to access systems to which the student has no authorization (i.e. hacking, spying, attempting to access proxies).
- Accessing or attempting to access, sending, or displaying offensive messages, pictures, or web sites (pornography or 'hate' sites).
- Employing the network for commercial use (i.e. selling video/music CDs, auction sites).
- Installing or attempting to install denial of service software (i.e. virus, sniffers).
- Stealing Fort Stockton ISD property (i.e. hardware, software, peripherals, etc.).
- Engaging in any activity which contravenes the laws of the United States or any other applicable jurisdiction.
- Connecting or attempting to connect personal computing devices to the FSISD network (i.e. PSP, Personal Laptops with broadband cards, cell phones or any other personal data devices).

14. **Consequences of *Improper Use - Student***

1st Degree Offenses—Student, parent, teacher, and administrator conference will be required to assess and correct the problem. Student will be assigned to detention, in-school suspension or other disciplinary measures at the administrator's discretion. The student/parent will be held financially responsible for any necessary repairs.
2nd Degree Offenses—Student, parent, teacher, and administrator conference will be required to assess and correct the problem. Student will be assigned to detention, in-school suspension or other disciplinary measures at the administrator's discretion. The student/parent will be held financially responsible for any necessary repairs.
3rd Degree Offenses—Student computer access privileges will be revoked for the remainder of the school year, and the student/parent will be held financially responsible for any necessary repairs. Loss of computer access privileges includes removal from all computer lab courses.

Habitual 1st or 2nd degree offenses can result in a 3rd Degree Offense consequence. Administrative action can include disciplinary or legal action including, but not limited to, criminal prosecution and/or penalty under appropriate state and federal laws. Improper or unethical use may result in the following disciplinary actions. Student actions not in compliance with the Student Acceptable Use Policy could result in:

a. User account to technology services restricted in part or whole or completely revoked
b. Restitution for costs associated with system restoration, hardware, software, etc.
c. Detention
d. In-school Suspension
e. Loss of class credit
f. Permanent removal from class and/or assigned an alternative class
g. Suspended or expelled from school
h. Alternate education assignment
i. Criminal charges filed
j. 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.

15. **Disclaimer** – The District's system is provided on "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.

STUDENT AUP

I have read the Fort Stockton ISD *Acceptable Computer Use Policy* and understand that the Internet account is designed for educational purposes only. I also understand that even though Fort Stockton ISD has an Internet filtering system, it is impossible for Fort Stockton ISD to restrict access to all controversial materials. I understand that I am responsible for my own actions on the Internet. I will not hold Fort Stockton ISD responsible for or legally liable for materials distributed to or acquired from the network.

As a student of Fort Stockton ISD, I agree to model appropriate computer etiquette and acceptable use of the network and proper network etiquette. Additionally, I agree to report any misuse of the information system to my teacher. I understand that misuse can come in many forms including, but not limited to, messages sent or received that indicate or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other issues described in the Fort Stockton ISD *Acceptable Computer Use Policy.*

I accept full responsibility for my actions when accessing the Internet. I hereby request an Internet account for myself, for educational and instructional use while a student of Fort Stockton ISD.

Print Name of **Student**_____

Campus _____ Grade _____

Signature of **Student**_____Date _____

STUDENT AUP
Permission to Display Work

Permission to display student work: I give FSISD permission to display my papers, projects, pictures, and/or electronic/video presentations to use on such medium including, but not limited to newsletters, school newspapers, documents, and/or the District web page. Only first names, if any names, will be used on the FSISD web page.

Mark one of the following boxes:

- ☐ **Yes**, I give my permission to display my work as described above
- ☐ **No**, I do not give permission to display my work as described above

Print Name of **Student**_____

Campus_____ Grade_____

Signature of **Parent/Guardian**_____Date _____