Friona ISD – Student Acceptable Use Policy

Introduction

Though there are a number of reasons to provide a user network access, by far the most common is granting access to students to enhance and continue their education. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the Friona Independent School District (FISD) network. This policy explains how FISD information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus students are asked additionally to use common sense when using FISD resources. Questions on what constitutes acceptable use should be directed to your Educational Mentor, your campus Principal, or the District Technology Director.

Friona ISD Technology Department Mission Statement:
Friona ISD will provide opportunities for all students to maximize potential and experience excellence.

To meet this challenge, the FISD Technology Department will:

- Structure a program that complies with the Texas Essential Knowledge and Skills as set forth by the Texas Legislature.
- Provide technology to students to continue and enhance their education.
- Assist teachers and students to integrate technology tools, including new technologies, techniques and skills in order to maximize future job potential.
- Better inform and utilize parents, community members and business leaders in the area of technology implementation.

All use of Friona ISD technology resources must be consistent with the policies and goals of the FISD School District, Texas Education Agency and Federal Education Initiatives.

Friona ISD controls student's access to inappropriate materials, as well as materials that are harmful to minors. FISD also makes every effort to ensure safety and security when using District-owned electronic communications including:

- Preventing unauthorized access, hacking and other unlawful activities.
- Restricting unauthorized disclosure, use and dissemination of personally identifiable information regarding students.
- Educating students about cyber-bullying awareness and response as well as appropriate online behavior.

Definition of FISD's Technology System: The District's computer system and networks are any configuration of hardware and software. The system includes, but is not limited to the following:

- Telephones (including wired, portable and mobile) and voicemail technologies
- Email accounts
- Servers
- Computer hardware and peripherals (such as scanners and printers)
- District-owned tablets and other portable devices
- Software including operating systems and application software
- Digital information including stored text, data files, email, digital images and audio/video files
- Internally or externally accessed databases, applications or tools (Internet or server-based)
- District-provided Internet access
- District-filtered student Wireless access
- New technologies as they become available

Always remember that access to the District's device, computer, network and Internet is a privilege, not a right.

General Guidelines

There is a lot of information in this document. A lot of do's and don'ts. You should read them all and be familiar with everything that is expected of you when using the FISD network and computers. However, here's a general idea of what you need to know:

- Use the network and all computer and tablet resources for educational purposes.
- Be safe, appropriate, careful and kind.
- Know that everything you do on the network is being monitored and retained.
- What you access on the Internet has to be filtered. You can't do anything to try to get around that filtering.
- Don't steal other people's work. Don't present another person's work as your own.
- Don't damage anything. This not only includes physical damage to computer hardware, but damage or theft of files and information as well.
- Always protect your privacy or your reputation. Don't do anything that hurts anyone else's privacy or reputation.
- Don't do anything illegal. There's a lot of things you can do out there and there's a lot of things you can't. Make sure you know the things that can get you in legal trouble and stay far away from them.
- Above all, always do what is right. You are expected to follow the same rules for good behavior and respectful conduct online AND offline. Respect yourself, respect your school.

Acceptable Use

Students will…

- use FISD provided technology for educational purposes. Games, websites, installed programs and any other accessible technology will be used under the supervision of a teacher or staff member, and will be used for educational purposes only.
- keep all passwords private and not share them with anyone, including other students.
- Students will follow all guidelines defined in this document for e-mail use, if issued a FISD e-mail account.
- keep in mind that all information viewed, sent and shared on any FISD technology device is logged and archived.
- only send, save or share files or information that they do not mind being made public. No privacy is implied for anything shared, saved or sent using the FISD network.
- use streaming media as allowed by their filtering rights, and with the understanding that bandwidth may be limited at times as deemed appropriate by FISD Administration.
- participate in District-approved social media learning environments related to curricular projects or school activities and use digital tools, such as, but not limited to, mobile devices, blogs, discussion forums, RSS feeds, podcasts, wikis, and on-line meeting sessions. The use of these resources is limited to the student's filtering rights and must be under the direct supervision of a FISD Teacher or staff member. The use of blogs, wikis, podcasts, and other digital tools are considered an extension of the classroom. Verbal or written language that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, wikis, podcasts, and other District-approved digital tools.
- Keep in mind that limited personal use of the FISD network shall be permitted if the use imposes no tangible cost to the district, does not burden FISD's computer or network resources, and has no adverse effect on the student's academic performance. Personal use may be limited or revoked by any FISD staff member at any time.

Unacceptable Use

Students will not:

- engage in activity that is illegal under local, state, federal, or international law.
- engage in any activities that may cause embarrassment, loss of reputation, or other harm to FISD.
- disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
- engage in activities that cause an invasion of privacy.
- engage in activities that cause disruption to the workplace environment or create a hostile workplace.
- use the network for any commercial activities including buying or selling services or merchandise, or making fraudulent offers for products or services.
- perform any of the following: port scanning, security scanning, network sniffing, keystroke logging, or other IT information gathering techniques.
- install or distribute unlicensed or "pirated" software.
- reveal personal or network passwords to others, including family, friends, or other members of the household.
- allow any other person use their name, logon, password or files for any reason (except for authorized staff members).
- store or display a printed password on their person or in or on personal items. Teachers and staff members may keep a list of printed passwords for students to reference. If handed to students, the student must give these passwords back to the teacher or staff member when finished using the network or online resource.
- use any sort of Peer-to-Peer file sharing sites for any purpose.
- use any Remote Desktop Access software
- circumvent FISD Security:
    - Students may not use FISD systems or devices to circumvent any security systems, authentication systems, user-based systems or to escalate privileges.
    - Students may not use any means to access passwords that are not assigned to them.
    - When on an FISD campus, students may not connect any devices to any network other than the FISD network.
    - use any means to disable the FISD Federally mandated filtering device.
- pretend to be someone else when posting, transmitting or receiving messages
- use inappropriate language including but not limited to swear words, vulgarity and racial slurs.
- waste school resources through improper use of FISD's technology resources, including creating and distributing chain letters, sending SPAM or using the network for any sort of financial gain.
- use the network to create or distribute hate mail, harassment, discriminatory remarks, pornographic references or graphics, cyberbullying and other related behaviors.
- post or transmit personal information about yourself such as addresses and phone numbers.
- respond to requests for personally identifying information or contact from unknown individuals
- make appointments to meet someone personally that was met originally online. If such a request is received it should be reported to a teacher or the campus Principal immediately.
- write, produce, generate, copy propagate or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of a computer's memory, file system or software. Such software is often called a bug, virus, worm or Trojan, among other names.
- alter or vandalize computers, networks, printers or other associated equipment and system resources.

- relocate or remove technology equipment (hardware or software) from its location without express written permission of the Technology Department.
- delete, examine, copy or modify files and data that belongs to another user.
- fraudulently alter or copy documents or files authored by another individual (Plagiarism)
- use any personal device without permission of FISD.
- FISD does not support personal equipment or software. Any use of personal equipment or software is covered by the FISD Portable Device Policy.

Illegal Activities

The following are considered illegal activities and are not allowed:

- Bullying
- Harassment
- Threats
- Obscene content
- Unauthorized Port Scanning
- Unauthorized Network Hacking
- Unauthorized Packet Sniffing
- Unauthorized Packet Spoofing
- Unauthorized Denial of Service
- Unauthorized Wireless Hacking
- Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
- Acts of Terrorism
- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statues
- Downloading, storing, or distributing copyrighted material

This list of illegal activities is not meant to be complete. All applicable Federal, State and Local laws are to be followed by staff and students of FISD. All violations will be reported to the appropriate law enforcement agencies and prosecution will be pursued as advised.

E-Mail

Personal usage of FISD email systems is prohibited. Users should use FISD email systems for district communications only.

- The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
- The user is prohibited from forging email header information or attempting to impersonate another person.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to FISD may not be sent via email, regardless of the recipient, without proper encryption.
- It is FISD policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.

All communications and information accessible via the FISD network, including those accessed outside FISD campuses, are to be considered private, and are the property of Friona ISD.

Forgery or the attempted forgery of e-mail messages is prohibited. Attempts to read, delete, copy or modify the e-mail of other users or the deliberate interference with the ability of others to send or receive e-mail is prohibited.

FISD requires additional parental permission and access for students to use district provided e-mail accounts who are 13 and younger. This permission and access also applies to the creation of non-school owned accounts, specifically Apple iTunes. A parent or guardian will be required to be present when these accounts are created and/or distributed, and will sign receipt of the account as well as any associated user names and passwords.

Network Access

Students should take all efforts to avoid accessing network data, files, and information that he or she has not been given express permission to access. Just because a student find that he/she has access to files or information does not imply or grant authorization to retrieve those files or information.

Blogging and Social Networking

Blogging and social networking by FISD students are subject to the terms of this policy, whether performed from the FISD network or from personal systems. Students may access blogs and Social Networking according to their filtering rights, and only with express permission from their supervising teacher or staff member. When using FISD hardware and/or software resources, students may only use and access blogs and Social Networking sites for educational purposes related to current classroom responsibilities. In no blog or website, including blogs or sites published from personal or public systems, shall material detrimental to FISD published. The student assumes all risks associated with blogging and/or social networking.

Web Browsing

Friona ISD filters student's access to the Internet according to the Children's Internet Protection Act (CIPA) which is Federal law. While FISD Administration and the FISD Technology Department work diligently to ensure inappropriate content is blocked, a chance still exists that a student may access unacceptable content. Students must report access to this content immediately (see **Reporting of Security Incident** below).

Copyright and Plagiarism

FISD's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner:

- copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's
- Posting or plagiarizing copyrighted material
- Downloading copyrighted files which employee has not already legally procured.

Students may not submit any assignment written fully or in part by any other individual. This includes, but is not limited to, other students, friends or family members, authors of free Internet sources, or commercial sites where writing can be purchased for a fee. Doing so is considered plagiarism and is subject to the FISD Student Code of Conduct.

Students will be required to maintain ethical and copyright standards in accordance with federal and state laws. No software will be loaded on a device without direct instruction from a teacher or FISD staff member. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

Privacy & Confidentiality

Students should expect no privacy when using the FISD network or FISD resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. FISD reserves the right to monitor any and all use of the computer network. To ensure compliance with FISD policies this may include the interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

Students will not disclose any information about another student or staff member without that person's permission, as well as the permission of the supervising teacher or staff member.

All networks run software that logs all activity on the FISD network. This includes, but is not limited to e-mail archiving, websites visited and images viewed. Law enforcement agencies can also track illegal activities back to the originating network (meaning back to FISD), and the logging software can then be used to locate the computer and the user where the illegal activity originated.

Respect for Privacy

I will respect my own privacy. I will not give out any information about myself or my family that may cause any harm. I will respect other's right to privacy and will not share any information about someone that may cause them harm or embarrassment. I will only access information that I have permission to access.

Personal Devices

All use of personal devices will be governed by the Portable Device Use Policy, as well as the Student Code of Conduct.

Personal Storage

FISD allows students to use personal flash drives on school devices to transfer acceptable files from school to home. Students must take precautions to ensure viruses, Trojans, worms, malware, spyware and other undesirable security risks are not introduced onto the FISD network.

Reporting of Security Incident

If a student knows of or suspects a breach of any security policy, the student must immediately notify his/her campus Principal, Homeroom Teacher, or Educational Mentor. Examples of incidents that require notification include:

- Any online bullying, threats or harassment, whether directed toward the student, or known by to the student to be happening to others.
- Suspected compromise of login credentials (password)
- Suspected virus/malware/Trojan infection
- Any attempt by any person to obtain a user's password over the telephone or by email
- Any other suspicious event that may compromise the security of FISD's network or information.

A student who gains access to any inappropriate or harmful material is expected to discontinue the access and to report the incident to the supervising staff member. Any student identified as a security risk or as having violated the Responsible Use Guidelines may be denied access to the District’s system.

Other consequences may also be assigned. Any violations of the use of the FISD network should be reported to the teacher, Principal or supervisor assigned to the student. Students who intentionally do not report violations will be considered to be in violation of the FISD Student AUP.

Software

Students will not install software without direct instruction from a teacher or FISD staff member. Installation of software must be under direct supervision of teacher or FISD staff member.

Vandalism

Vandalism is defined as any malicious attempt to harm or destroy physical property or the data of another user. Vandalism also includes willfully changing any setting on a device owned by FISD to circumvent security or to bypass filtering required by federal law.

Users shall not alter or vandalize computers, networks, printers or other associated equipment and system resources. Alteration or vandalism includes, but is not limited to, removal of parts, intentional destruction of equipment, attempting to degrade or disrupt system performance, or attempting to make system resources unusable.

Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system(s), or any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to compromise, degrade, or disrupt system performance may be viewed as violations of District policies and administrative regulations and, possibly, as criminal activity under applicable state and federal laws.

Access and Bandwidth

Excessive use of FISD bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low FISD-wide usage.

Enforcement

This policy will be enforced by FISD Administration at the campus and district level. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including expulsion. Where illegal activities or theft of FISD property (physical or intellectual) are suspected, FISD may report such activities to the applicable authorities. FISD students are solely responsible for all legal ramifications of their actions on the FISD network, including, but not limited to, any fines, fees or mandated restitution that may be incurred.

The district will cooperate fully with local, state or federal officials in any investigation concerning or relating to the misuse of the District's electronic communication system.

A student who knowingly brings prohibited materials into the school's electronic environment will be subject to disciplinary action according to the Student Code of Conduct.

Closing

This document is a part of FISD's cohesive set of student policies. Other policies, especially the Student Code of Conduct, may apply to the topics covered in this document. Any applicable policies will be reviewed and implemented as needed.

The district shall not be liable for student's inappropriate use of FISD's network or e-mail resources. FISD is not responsible for student's copyright infractions, mistakes or negligence or costs incurred by students. The district shall not be responsible for ensuring accuracy or usability of any information found on the Internet. The Superintendent with the help of the District Technology Director will oversee FISD's network and communication resources. FISD's systems will only be used for administrative and educational purposes consistent with the District's mission and goals.

FISD's network and computer system is provided as an "as is" and "as available" basis. The District does not make any warranties, whether expressed or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not guarantee that the functions or services performed by, or that the information or software contained on the system will meet the system 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.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

Please Print:

Student Name:

Student Grade:	Student ID:

Signatures:

Student Signature:

Parent/Guardian Signature:
