Fredericksburg ISD
Cybersecurity Policy
2019-20

Purpose

This cybersecurity policy is for Fredericksburg ISD (FISD) employees, students, vendors, and partners. The purpose of this policy is to protect sensitive data, student records, direct/indirect identifiers, and technology infrastructure. This policy applies to all if FISD's employees, vendors, partners, and students who have access to systems hardware and software.

Fredericksburg ISD technology department is obligated to conserve and protect FISD resources for the benefit of the public interest rather than their private interests; however, the responsibility and accountability for the appropriate use of FISD resources ultimately rests with the individual who uses the resource or who authorizes such use. The intention of the following policies are to preserve and enhance the integrity of those resources. Noncompliance with this agreement will result in disciplinary action consistent with District Policies and Regulations and/or, if appropriate, termination of contracts and services with the district. Violations of the law may result in criminal prosecution and/or disciplinary action by the district.

Definitions

FISD resources include electronic and communications equipment, software, and systems, including but not limited to computers, laptops, iPads, computer networks, software, copiers, scanners, printers, connected classroom equipment, other computer peripherals, cellular phones, applications such as the internet, email, office systems under the individual's control or to which they have access.

Cyber attack means an attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.

Cybersecurity means the measures taken to protect a computer, computer network, or computer system against unauthorized use or access.

Compliance with Children's Internet Protection Act (CIPA)

FISD does not condone inappropriate behavior while online, including cyberbullying, and will take appropriate disciplinary actions in response to that behavior.

Availability of Access

Access to FISD Resources, including the internet, shall be made available to users primarily for instructional and administrative purposes and in accordance with administrative regulations.

Limited personal use of the network shall be permitted if the use imposes no tangible cost to the District, does not unduly burden the District's computer or network resources and has no adverse effect on an employee's job performance or on a student's academic performance.
Users will communicate via e-mail on District equipment through their assigned @fisd.org/@student.fisd.org email account only. All guest access will be obtained via the district's BYOD network which includes an acceptable us agreement.

Fredericksburg ISD
Cybersecurity Policy
2019-20

Monitoring and Use

FISD reserves the right to monitor the activities of all individuals using FISD resources, to include but not limited to, computers, e-mail, internet, and any other electronic equipment connected by any means to FISD's network. Cellular phones, when connected to FISD's network are also subject to monitoring. Users shall have no expectation of privacy when using FISD resources. Items to be posted on the FISD network, including but not limited to web sites, will be screened prior to posting.

Disclaimer of Liability

FISD shall not be liable for the users' inappropriate use of the District's resources, violations of copyright restrictions, users' mistakes or negligence or costs incurred by users. FISD shall not be responsible for ensuring the accuracy of usability of any information found on the Internet. Additionally, FISD shall not be liable for users encountering objectionable material whether accidentally or purposefully.

Copyright

Users of FISD resources are required to comply with all copyright laws. Copyrighted software, data or other file types may not be placed on any system connected to FISD's network without permission from the holder of the copyright and the Technology Director.

Network Security

FISD's network security measures are to protect against cyber attack. The users of FISD resources will not physically connect or attach any unauthorized hardware or equipment to the network. This prohibition includes but is not limited to laptops, cell phones, portable hard drives or other computers designated for "stand alone" operations. However, personal data devices such as listed above may connect wirelessly to the FISD BYOD network. Texas Penal Code section 33.02, Breach of Computer Security, allows for prosecution up to first degree felony for a person who "…knowingly accesses a computer, computer network, or computer system without the effective consent of the owner." Other than FISD property, the only equipment allowed to connect physically to any FISD network, other than BYOD, is a USB Flash Drive.

FISD network managers will ensure the maintenance of a content filter, firewall, security settings within the network, password provisions, software and hardware updates, adherence to SFTP protocols, antivirus software, and the education of the end user on practices for cybersecurity safety.

Fredericksburg ISD
Cybersecurity Policy
2019-20

Network Access

Users are responsible for the security of electronically stored information (data) to which the user's account has been given permission to use. All users given permission to access data must act in a manner to protect said data from loss, unauthorized alteration or unauthorized use. Unauthorized use of an FISD computer account is prohibited.

Computer accounts are assigned to individuals for their exclusive use. Users are responsible for all activities conducted with the account assigned to them. Level of access to the network is determined at the time the account is established according to the status of the user (e.g. student, teacher, or administrator) and requirements to access specific data. Request for changes in access level may be made through the Technology Director.

Data will not be copied or transmitted without the same access restrictions as those placed on the original data. Users are responsible for data accessed, transmitted, copied, deleted or changed using their account.

Network Etiquette

You are expected to abide by the generally accepted rules of network etiquette. This includes (but is not limited to) the following:

a. General school rules for adequate behavior apply just as they do in classrooms and hallways. Be polite. Do not send jokes or other comments that may be discriminatory, harassing, or offensive to others, or material that defames an individual, company or business or disclose personal information without authorization.

b. Criminal speech, dangerous information, and other illegal activities are strictly forbidden. School harassment regulation apply to electronic communications. Additionally, Texas Penal Code makes many of these actions criminal in nature.

c. Do not reveal your name, personal address or phone number or those of your colleagues.

d. Note that Internet and e-mail usage is not guaranteed to be private. The district will have access to all mail as well as sites visited. Messages relating to or in support of illegal activities may be reported to the authorities.

e. Do not use the network in such a way that you would disrupt the use of the network by other users.

f. All communication and information accessible via the network are subject to copyright and other laws.

g. Do not attempt to bypass the internet filter to obtain inappropriate information or for any other reason.

User responsibilities

1. User accounts belong to the person to whom it is issued and ONLY that person is authorized to use it. Users do not have the right to allow another person to use their account. Users are responsible for all actions taken by their account at all times.

2. Gaming and other bandwidth intensive uses, such as Internet music or video are not allowed. In order to ensure smooth system operations, the system administrator has the authority to monitor all accounts.

3. FISD resources, especially computers, monitors and printers, are assigned to a specific location and are not to be moved without the express permission of the Technology Director.

4. FISD reserves the right to block access to certain Internet Sites. Access is blocked at multiple locations. Attempts to circumvent these restrictions via proxy sites or other methods can result in loss of the individual's account. If damage is incurred while bypassing or attempting to bypass FISD restrictions, criminal charges may be filed.

5. Users are legally and ethically responsible for protecting and preserving FISD's proprietary rights. This means that no messages disclosing sensitive, confidential, restricted, non-public or other proprietary information may be transmitted over the online system.

6. Users should use FISD resources in a businesslike, courteous and civil manner. All FISD policies, including policies prohibiting discrimination and sexual harassment shall apply to use of FISD resources. FISD resources shall not be used for the expression of unlawful or discriminatory ill will or bias against individuals or groups, or offensive material such as obscenity, vulgarity, or profanity. Additionally, FISD resources will not be used for political purposes, to include e-mailing political representatives.

7. Users should exercise due care to ensure that spyware, viruses, Trojan Horses and other malware are not introduced to the network. At the first indication that malware is present, the user should stop using the computer and contact the Technology Department immediately. Users will not resume using that equipment until expressly given permission to do so by the Technology Department.

8. FISD reserves the right to withdraw account privileges at any time for any reason. Additionally, accounts will be disabled upon the user's disassociation with FISD.

9. Use of instant messaging technology is prohibited unless permission is granted by the Technology Director based on necessity to accomplish FISD's educational mission.

Users who violate these standards may be subject to disciplinary action in accordance with District policy and/or legal requirements.

Cyber attacks and vandalism

Cyber attacks are prohibited. Additionally, deliberate attempts to physically damage, compromise, degrade or disrupt system performance shall be viewed as violations of District policies and administrative regulations and, possibly, as criminal activity under applicable state

and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Forgery Prohibited

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of another network user or deliberate interference with the ability of other network users to send/receive electronic mail is prohibited.

Warning

Network users and parents of students with access to FISD resources should be aware that use of the network may provide access to other electronic communication systems in the global electronic network that may contain inaccurate or objectionable material.

Disclaimer

FISD resources are provided on an "as is, as available" basis. The District does not make any warranties, expressed or implied, with respect to any services provided by the network and any information or software contained therein. The District does not warrant that the functions or services performed by, or 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 network users, information providers, service providers, or other third party individuals in the network are those of the providers and not the District.

The district will provide notice to the parties involved or affected by any cybersecurity incident involving personal information.

The district is not responsible for cyber attacks or cybersecurity breaches that involve third party vendors.

FISD will cooperate fully with local, state or federal officials in any investigation concerning or relating to any cybersecurity attack or other cybersecurity incident against the cybersecurity infrastructure at FISD.