General Security – Acceptable Use Policy

Policy Title	Acceptable Use Policy
Policy Category	IT – Security Policy
Policy Owner	Information Technology
Policy Approver(s)	Chief Information Officer or Designee
Related Policies	Student Code of Conduct; Employee Handbook
Related Procedures	N/A
Effective Date	July 1, 2022
Next Review Date	June 2023

Purpose

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

Access to the Districts' electronic communications systems which may include computers, software, communication tools (email, chat), access to internal networks (intranet), and access to external networks (internet) is a privilege, not a right. Fort Worth ISD requires that these systems be used in a responsible way, ethically, and in compliance with all legislation and other Fort Worth Independent School District (District) policies. [See Board Policy CQ]

All users shall be required to acknowledge receipt and understanding of all administrative regulations governing the use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations and guidelines may result in suspension or terminations of privileges and other disciplinary action consistent with District Policies. [See Board Policies DH and CQ, and the Student Code of Conduct]

Scope

This policy is applicable to all District stakeholders including full-time, part-time, and temporary employees, contractors, students, and interns. The requirements defined in this policy are applicable to all data, systems, and services owned and/or managed by the District.

Electronic mail transmissions and other use of the electronic communication system by students and employees shall not be considered confidential and may be monitored at any time by designated District staff.

Definitions

- **Shadow IT:** The acquisition and use of information technology systems and/or services within the organization that has not been approved by the IT Department. Oftentimes, the IT Department is not even aware of these solutions being implemented.
- **Malware:** A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or of otherwise annoying or disrupting the victim.
- **Social engineering:** The "con game"; the art of manipulating end-users into providing confidential or personal information. One example is "phishing," where hackers pretend to be trusted organizations such as banks, company suppliers, IT staff, or mobile carriers to get your personal information such as credit card details or confidential corporate information.
- **Removable media:** Any type of storage device that can be removed from a computer while the system is running. Examples include USB flash/thumb drives, memory cards, CDs/DVDs, external hard drives, or mobile devices used for storage purposes such as smartphones. While there are business purposes for these devices, they are also known to be common sources of malware infections and susceptible to loss or theft, leading to breaches of sensitive information.
- **Service Desk:** The Fort Worth Independent School District internal service desk support team can be reached by phone at (817) 814-4357.

Policy

A. Acceptable Use of Assets

Assets include, but are not limited to, physical equipment, such as desktop computers, servers, printers, laptops, telephones, mobile devices, and removable media (such as USB flash drives), as well as systems and services, such as the organizational network, internet, voicemail, and more. Organizational data is also considered to be an asset. All devices and systems are property of the District and all use must be in accordance with established policies, standards, and guidelines.

1. The District allows limited use of the network, systems, and devices for personal reasons (personal correspondences, online banking, etc.), but personal use must not be abused. Personal use is acceptable provided it is limited to the following considerations:
    a) It does not have a negative impact on overall productivity.
    b) It does not cause additional expense to the District.
    c) It does not compromise the District in any way.
    d) It does not disrupt the network performance in any way.
    e) It does not, in any way, contradict any other District policies, standards, and/or guidelines.
2. District assets and systems may not be used for illegal or unlawful purposes, including copyright infringement, obscenity, personal gain, libel, slander, fraud, defamation, plagiarism, intimidation, forgery, impersonation, illegal gambling, soliciting for pyramid schemes, and computer tampering (e.g., spreading computer viruses).
3. Users should not access and/or purchase technology, devices, applications, or services that are not formally authorized and approved by IT. (This circumvention of the IT Department is known as Shadow IT.)
4. IT assets, such as laptops and mobile devices, are intended to be used only by the people to whom they have been issued. If an unauthorized person is using the device, the use should be monitored to ensure that no sensitive data is accessed by the unauthorized party. The person to whom the device was issued is ultimately responsible for any actions performed with the device.

5. Users will protect District IT assets, keeping them physically and logically secured and under the control of the user, including but not limited to:
    a) Locking down laptops with a locking cable or storing them in a locked drawer or cabinet when leaving them in the office.
    b) Ensuring the workstation is locked (screen/keyboard) whenever walking away from it.
6. Access to District systems and devices is controlled through individual accounts and passwords. Users are responsible for not sharing the password for that account with others.
7. As applicable, you must comply with the District's record management program, the Texas Open Meetings Act, the Public Information Act, the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student and District records, and campaign laws.

B. Electronic Communication and Internet Use

The use of District communication and internet systems and services (including email, instant messaging, voicemail, forums, social media, and more) is provided to perform regular daily tasks. The use is a privilege, not a right, and therefore must be used with respect, common sense, and in accordance with the following requirements:

1. The email systems and other messaging services used at the District are owned by the District and are therefore its property. This gives the District the right to monitor any and all email traffic passing through its email system. This monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the email system, review by the HR and legal team during the email discovery phase of litigation, and observation by management in cases of suspected abuse or employee inefficiency.

2. The District often delivers official communications via email. As a result, employees of the District with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important District announcements and updates, as well as for fulfilling business and role-oriented tasks.

3. Electronic communication and the internet must not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment (including offensive and/or insulting content), discrimination, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading computer viruses).

4. District communication platforms and the internet are not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g., emailing large attachments instead of pointing to a location on a shared drive). Individual use of resources will not interfere with others' use of the District email system and services.

5. Users are prohibited from using accounts that do not belong to them and are prohibited from using platforms to impersonate others.

    a) Users are not to give the impression that they are representing or providing opinions on behalf of the District unless otherwise authorized.

6. Users shall not open message attachments or click on hyperlinks sent from unknown or unsigned sources through any platform (email, instant message, social media, etc.). Attachments/links are the primary source of malware and social engineering and should be treated with utmost caution.

7. The District prohibits the use of email or other messaging platforms for mass unsolicited mailings, chain letters, and competitive commercial activity unless preapproved by the District.

8. Any allegations of misuse should be promptly reported to the Service Desk. If you receive an offensive or suspicious email, do not forward, delete, or reply to the message. Instead, report it directly to Service Desk.

9. Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to unsubscribe from the list and is responsible for doing so if their current email address changes.

10. Archival and backup copies of email messages may exist, despite end-user deletion, in compliance with District's Records Retention Policy.

11. Email access will be terminated when the user terminates their association with the District, unless other arrangements are made. The District is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their relationship has ceased.

12. Users shall not send sensitive information that is not appropriately protected (encrypted). (Appropriate means of protection include but are not limited to OneDrive or encrypted attachments through email.)

    a) Users shall take extra precautions when transmitting District, client, and/or other regulated information via electronic communications. Sensitive material should be marked and encrypted appropriately. Keep in mind that all email messages sent outside of the District become the property of the receiver.

13. Users are not permitted to automatically forward emails received by their District account to an external email address or another messaging system.

14. THE DISTRICT ASSUMES NO LIABILITY FOR DIRECT AND/OR INDIRECT DAMAGES ARISING FROM THE USER'S USE OF THE DISTRICT'S EMAIL SYSTEM AND SERVICES. USERS ARE SOLELY RESPONSIBLE FOR THE CONTENT THEY DISSEMINATE. THE DISTRICT IS NOT RESPONSIBLE FOR ANY THIRD-PARTY CLAIM, DEMAND, OR DAMAGE ARISING OUT OF THE DISTRICT'S EMAIL SYSTEMS OR SERVICES.

15. Email users are expected to remember that email sent from the District's email accounts reflects on the District. Email users must comply with normal standards of professional and personal courtesy and conduct.

16. Users shall not attempt to bypass the District's web filter through the use of any technologies or third-party browsers. Attempts to do so violate the acceptable use policy and all of the User's privileges may be revoked as a result of such a violation.

C. Security Unacceptable Uses

The IT Department will manage security policies, network, application, and data access centrally using whatever technology solutions are deemed suitable. Any attempt to contravene or bypass security will be deemed an intrusion attempt and will be subject to disciplinary action. The following restrictions and requirements are enforced at the District to establish and maintain the confidentiality, integrity, and availability of systems and data:

1. Users must not introduce malicious programs into the network or a system (e.g., viruses, worms, Trojan horses, email bombs, etc.).

2. Users must not introduce or contribute to security breaches or disruptions of network communication.

a) Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a system or account that the user is not expressly authorized to access unless these actions are within the scope of regular duties. For the purposes of this section, “disruption” includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

3. Port scanning or security scanning is expressly prohibited unless prior authorization is granted in writing by the Chief Information Officer.

4. Users must not execute any form of network monitoring that will intercept data not intended for the user’s host unless this activity is a part of the users’ daily activities.

5. Users must not circumvent user authentication or security of any host, network, or account.

6. Users must not introduce honeypots, honeynets, or similar technology on the corporate network.

7. No servers (i.e., running web or FTP services from user workstations) or devices that actively listen for network traffic are allowed to be put on the corporate network without prior written authorization by the Chief Information Officer.

8. Users must not interfere with or deny service to any user (for example, denial of service attack).

D. Ownership and Privacy Issues

The systems are the District’s property as well as, for access and security purposes, the information they contain. We respect our users’ right to privacy; however, we grant access to our systems for business and educational use. Users must not expect that information contained in these systems is private. The District reserves the right, from time to time, for legal, or otherwise valid reasons, to read, monitor, control, and access user files and messages created, saved, transmitted, or received. In the event of intercepted illegal activity, we will bring them to the attention of the appropriate authority without prior notification to the sender or receiver.

E. Noncompliance

Violations of this policy will be treated like other allegations of wrongdoing at the District and will be investigated per established procedures. Sanctions may include, but are not limited to, one or more of the following:

1. Oral and/or written warning
2. For Employees: Probation, suspension, or termination of employment
3. Discipline in accordance with the Student Code of Conduct
4. Legal action per applicable laws and contractual agreements

By signing below, I acknowledge that I have read, understand, and agree to abide by the provisions of the Acceptable Use Policy of the Fort Worth Independent School District.

Date: _____ School / Location: _____

Name: _____ Signature: _____

Parent/Legal Guardian Name: _____ Parent/Legal Guardian Signature: _____