Shawnee Heights Fire District

TELECOMMUNICATIONS POLICY

Purpose: To establish a policy on the use of the District's information technology systems.

Applicability: To all District employees.

Effective Date: November 20, 2008

1. SCOPE
    a. This policy applies to employees, agents, contractors, sub contractors, consultants, vendors, service providers, and temporary workers [collectively, "users"] on District premises or using the District's information technology systems.
2. ACCEPTABLE USE
    a. Users are granted the use of the District's information technology systems that include all types of computerized equipment including but not limited to:
        i. Hand-held devices
        ii. PDA's
        iii. Computer applications and tools
        iv. Office systems
        v. Network facilities
        vi. Telephone systems
        vii. Wireless systems
        viii. Cellular telephones
        ix. Radios and pagers
    b. Users are also granted access to the Internet, Intranet, World Wide Web, email, and other applications through use of the District's information technology systems. The use and access are granted for business purposes of the Shawnee Heights Fire District.
    c. The use and access may be denied at any time, for any reason. Users are responsible at all times for using the information technology systems in a manner that is ethical, legal and consistent with the best interests and policies of the District.
    d. The information technology systems are intended for the business use by the District. The District understands that employees may, from time to time, wish to use the systems for personal matters. While such use is not strictly prohibited, it must be reasonable, limited, and consistent with District policies. Such use should not interfere with the District's business, interfere with the user's ability to perform his or her job, interfere with the ability of others to perform their jobs, expose the District to liability or embarrassment, be for any of the Prohibited Uses as stated below, violate the laws of the location information is transmitted to or from, or violate any policies of the District.
    e. Only users who are authorized by the District may use the District's systems. A user may not allow any other person, including authorized users, to access any application through the user's account profile.

3. USER RESPONSIBILITY
    a. Users are responsible for any and all activity initiated from their accounts or profile. Therefore, users should protect their passwords, change them regularly, not revel them to others, change their passwords whenever disclosure has occurred or may have occurred, and not leave their computers on and open for non-authorized users to access. Users are responsible for protecting their own files (email, word processing, spreadsheets, etc.) from unauthorized persons.
    b. If a user inadvertently accesses another user's files, the user must immediately discontinue access, report the access and refrain from revealing any personal information discovered.
    c. Users are hereby advised that there is material on the Internet that is offensive to most people. The District does not have the ability to control this information, and does not attempt to screen it all. Users must use their good judgment and common sense to stay away from offensive Internet sites. The District disavows any liability from harassment by any person who uses a District system and is offended upon discovering such offensive material.
    d. Users will attach the following as a footer to all emails sent from a District system or when sending emails that contain District information from another system.
        i. The information contained in this electronic document and any attachments is privileged and confidential. If you are not the intended recipient or authorized to retrieve messages for the intended recipient, you are hereby notified that any dissemination, distribution or duplication of this information is strictly prohibited. If you have received this communication in error, please notify me immediately and completely delete this document and any attachments from your system(s). If you are the intended recipient, but do not wish to receive communications through this medium, please advise me immediately.

4. NO RIGHT TO PRIVACY
    a. All information created, accessed, or stored using the District's applications and information technology systems is the property of the District. Users do not have a right to privacy to any activity conducted using the District's information technology systems. Representatives of the District can review, read, access or otherwise monitor all activities on District systems or on any other system accessed by use of a District system. The District monitors web sites that are visited.

5. PROHIBITED USES
    a. Sales and Solicitation
        i. Users may not send email for any purpose other than personal communication. Users may not transmit unsolicited commercial or bulk email or advertise or offer to sell goods or services to others. Unless approved by the Fire Chief or his designates, users may not use the system for soliciting funds for school fundraising drives or selling products or merchandise or to solicit political support. Users may not use District information systems to make fraudulent offers to sell or buy products, items, or services. Users may not use District information systems to advance any type of financial scam such as pyramid schemes, Ponzi schemes or chain letters.
    b. Confidential Information
        i. Users must not use email or any other method to send District proprietary or confidential information to nay unauthorized person. Such information may be sent to authorized persons in encrypted files if sent over publicly accessible media such as the Internet or broadcast media such as wireless communication.

Such information may be sent in unencrypted files only within the District's system.

c. Deception
    i. Users may not intercept or attempt to intercept email or network traffic, attempt to access the accounts of others, or attempt to penetrate the security measures of the District. This includes, but is not limited to, intentionally seeking information on, obtaining copies of, or modifying files, email or other data or passwords belonging to other users without their express permission.
    ii. Users may not send, or cause to be sent, communications that make use of or contain invalid or forged headers, invalid or non-existing domain names or other means of deceptive addressing. Similarly, email that is relayed through a third party's mail server without the permission of that third party, or which employs similar technologies to hide or obscure the source of the email is unauthorized. Users may not impersonate another user by modifying email header information, or otherwise hide the user's identity.

d. Nuisance Email and Email Attachments
    i. No unexpected email attachments received from unknown persons should be opened. Doing so leaves the District vulnerable to viruses, and also may violate application licensing agreements or copyright laws. Users may not create or forward nuisance email, including jokes and chain letters.

e. Software Installation, Downloads, and Banned Software
    i. No software, games or other applications may be installed or downloaded on a District system without the Fire Chief's authorization. Users may not make copies of applications running on District systems for use at home, on laptops or for other reasons, without authorization.
    ii. Users may not knowingly download or upload, email, install, or post files that contain software, music, video, or other material protected by intellectual property laws, rights of privacy or publicity, copyright, trademark, patent, trade secret or any other applicable law unless the user owns or controls the rights to or has received all necessary consents.
    iii. Instant messaging software, file sharing and peer-to-peer (P2P) programs, multiplayer games, or any software that automatically accesses the Internet from the user's computer is prohibited. Examples of banned software include, but are not limited to, AOL Instant Messenger, Yahoo Instant Messenger, Weather Bug, Webshot, Kaaza, Imesh, and Limewire.

f. Modems
    i. Any computer connected to the District's network cannot contain or connect to a modem or any similar device without the approval of the Fire Chief.
g. Illegal Uses
    i. Users are prohibited from using the District's information systems for wagering or betting.
    ii. Users shall never harass, intimidate, stalk, threaten others or engage in other illegal activity (including pornography, terrorism, espionage, theft or illegal drugs) by email or other methods. It is specifically prohibited for users to knowingly visit sites that feature pornography, terrorism, espionage, theft or illegal drugs.
    iii. Users must not abuse or violate the legal rights of others. All such activities should be reported to management for appropriate action.
    iv. Users may not publish, post, distribute or disseminate defamatory, obscene or unlawful material or information via the Internet, or violate any applicable local, state, national or international law.

6. VIOLATIONS
    a. Violation of this policy may result in discipline up to and including termination of employment.

THIS POLICY SPECIFICALLY REPEALS AND REPLACES PRIOR DISTRICT POLICIES AND ADMINISTRATIVE MEMORANDA RELATIVE TO TELECOMMUNICATIONS.

Approved: By Board Action on November 20, 2008.

EMPLOYEE ACKNOWLEDGEMENT

I have read and understand the Shawnee Heights Fire District's Telecommunications Policy. Specifically, I acknowledge my understanding of the following:

1. I understand the type of conduct and behavior that is prohibited under this policy.

2. I understand that I will be subject to discipline, up to and including the termination of my employment, if I engage or conduct prohibited by this policy.

3. I know how to report violations of this policy to the Shawnee Heights Fire District.

_____ _____

Signature Date

_____

Printed Name