CITY OF FRISCO PERSONNEL POLICIES
COMMUNICATION AND COMPUTER POLICY

Subject:	**COMMUNICATION AND COMPUTER ACCEPTABLE USE POLICY**	**Date:**	**11/06/2007**
		Revision Date:	**12/01/2020**
Approved by Ordinance:	**07-11-56**	**Revised by Ordinance:**	**2020-12-77**

I Statement of Purpose:

This policy outlines the appropriate use of all electronic and telephonic communication systems, including, but not limited to, computers, telephones, the internet, e-mail, voice mail, pagers, and all communications and information transmitted by, received from, or stored in City of Frisco ("City") owned or leased systems.

II Scope:

This policy applies to employees, contractors, consultants, temporaries, and other workers at the City, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City.

III Policy:

City Property. All Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, telephone equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP are the property of the City and, as such, are to be used for purposes related to an individual's job with the City, subject to exceptions noted below. For security and network maintenance purposes, authorized individuals within the City may monitor equipment, systems and network traffic, including, but not limited to, network accounts providing electronic mail, at any time. The City reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

The City shall not be liable for users' inappropriate use of electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The City shall not be responsible for ensuring the accuracy, age, appropriateness, or usability of any information found on electronic resources, including the Internet.

The City's system is provided on an "as is, as available" basis. The City does not make any warranties, whether express 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 City uses a variety of vendor-supplied hardware and software. Therefore, the City does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements. Neither does the City 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 City. The City will cooperate fully with local, state, or federal officials in any investigation concerning, or relating to, misuse of the City's electronic communications system.

Personal Use. The City allows incidental and occasional personal use of the communication systems covered by this directive provided that such use does not adversely affect City business uses and/or productivity and does not involve unlawful or unprofessional activities. Incidental and occasional personal use of the systems is allowed during non-working hours (before work, during lunch and after normal working hours) only to the extent such use: 1) imposes no tangible cost on the City; 2) does not unduly burden the City's computer or network resources; and 3) has no adverse effect on an employee's job performance. When an emergency requires an employee to make or receive personal calls during business hours, every attempt should be made to limit the calls to five (5) minutes. City communication systems including email, shall not be used to conduct personal business.

Personal Bills Incurred. The Department Director must authorize, in advance, personal long-distance calls made by an employee and billed to the City, and the employee must reimburse the City for whatever charges are incurred. The same rules will apply to computer systems. Should an employee incur any charges on the computer system or the Internet, he/she must have advance permission and must reimburse the City for those charges within 30 days of when the fee was charged. Any fees not reimbursed will be deducted from an employee's monthly compensation and/or final paycheck from the City.

Security and Confidential Information. User accounts are not to be shared. Passwords must be kept secure and adhere to the City Password Policy. All systems, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by locking the system when the host will be left unattended. Postings by an employee from a City email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the City, unless posting is in the course of business duties. All hosts used by the employee that are connected to the City Internet/Intranet/Extranet, whether owned by the employee or the City, shall be continually executing approved virus-scanning software with a current virus database unless granted an exception by the

Information Technology Department. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. The Director should monitor departmental use of the Internet and e-mail, and he/she may revoke an employee's access to such systems at any time.

Privacy and Open Records. An employee does not have a privacy right in any matter created, received, or sent via City-owned or leased systems. The City reserves the right, without advance notice, and at any time, to monitor, access, delete, or disclose any messages or documents created, received, sent, or stored via the City-owned or leased systems. The City is subject to open records requests and any information on a City computer may be subject to the right of discovery through the Texas Public Information Act.

Program Installation. All programs installed on computers must be fully licensed for that computer. No personal or downloaded programs are to be installed unless granted an exception by the Information Technology Department.

IV Internet and E-mail Usage:

Discrimination and Harassment. Creating, sending, forwarding, or storing Internet or e-mail messages or documents (including, but not limited to, e-mail message signature lines, sayings and quotations) which are offensive, intimidating, harassing, disparaging, or hostile on the basis of race, color, religion, sex (including pregnancy, sexual orientation, and gender identity), age, national origin (including citizenship), veteran status, disability and genetic information as designated by all relevant laws and regulations is grounds for disciplinary action, up to and including termination. The City does not allow connections to sites that contain sexually explicit material. Use of such sites on City-owned or leased equipment may lead to disciplinary action up to and including termination.

Open Records and Privacy. Electronic messaging systems as well as other computer systems are subject to the right of discovery in legal actions brought against the City and through the Texas Public Information Act. This means that outside parties may have access to the information stored on the City's systems and, as a result, such information may become public knowledge through no action of the City. Additionally, each employee should assume that every Internet site that is visited would capture his/her electronic address, which can lead back to the City.

Unacceptable Use. The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of the City authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing City resources. The lists below are by no means exhaustive but constitute an attempt to provide a framework for activities which fall into the category of unacceptable

use.

V System and Network Activities:

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or City protected by copyright, trade secret, patent, or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by City.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which City or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a City computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any City account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior approval from the Information Technology Department is received.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Interfering with, or denying service to, any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command or sending messages of any kind with the intent to interfere with, or disable, a user's terminal session, via any means, locally, or via the Internet/Intranet/Extranet.

- Providing information about, or lists of, City employees to parties outside City.
- Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages, whether public or private.
- Using the network for financial gain or for commercial activity.

Email and Communication Activities:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within City's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by City or connected via City's network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Attempting to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person’s user ID and/or password is prohibited.

Blogging:

- Blogging by employees, whether using City’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of City’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate City’s policy, is not detrimental to City’s best interests, and does not interfere with an employee's regular work duties. Blogging from City’s systems is also subject to monitoring at any time.
- City’s employees are prohibited from revealing any City confidential or proprietary information when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation, and/or goodwill of City and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by City’s Discrimination and Sexual Harassment policies.
- Employees may also not attribute personal statements, opinions, or beliefs about the City when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or

implicitly, represent themselves as an employee or representative of City. Employees assume any and all risk associated with blogging.

- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, City's trademarks, logos, and any other City intellectual property may also not be used in connection with any blogging activity.

VI Illegal Activities:

Employee use of the City owned or leased electronic and telephonic communication systems, including telephones, the Internet, e-mail, voice mail, and pagers must comply with all other Administrative Directives of the City and any established departmental policies. Illegal activities discovered by monitoring or auditing activities may be brought to the attention of the appropriate governmental agency or other persons.

Improper or unethical use may result in disciplinary actions consistent with City policies and procedures and, if appropriate, the Texas Penal Code, Computer Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs.

VII Enforcement:

Access to the City's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to comply with such regulations and guidelines. Noncompliance with applicable regulations may result in suspension or termination of privileges and other disciplinary action consistent with City policies. Violations of law may result in criminal prosecution as well as disciplinary action by the City, up to an including termination of employment.

VIII Definitions:

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Host	A machine that communicates via a network, includes servers and clients.
Ponzi	A fraudulent investment operation that involves paying abnormally high returns ("profits") to investors out of the money paid in by subsequent investors, rather than from net revenues generated by any real business. It is named after Charles Ponzi.
Trojan Horse	A program that installs malicious software while under the guise of doing something else.
Worm	A program that replicates itself over a network and usually performs malicious actions.
E-mail Bomb	Sending huge volumes of e-mail to an address in an attempt to overwhelm a system.