City of FRESNO

ADMINISTRATIVE ORDER NUMBER 8-11

SUBJECT: Use of Electronic Systems & Tools

Responsible Department: Information Services (ISD)
Date Issued: 07-24-2007
Date Revised: 01-14-2020
Approved: *(Signature on File)*

Purpose

The purpose of this policy is to establish the proper use of electronic equipment, systems and/or tools provided by the City of Fresno (City) to its employees for the purpose of performing job functions including communication, information exchange and research.

Definition

Electronic systems are defined as: All hardware (computers, laptops, tablets, smartphones, Global Positioning Systems (GPS), etc.), software and tools owned by the City and available for official use by City employees, including but not limited to, electronic mail, voice mail, calendaring, texting, messaging, social media sites and the Internet.

Policy

The following policy outlines the policy for the use of Electronic Systems and Tools for the City of Fresno.

Ownership

All electronic systems, temporary or permanent files, and any related systems or devices are the property of the City. These include, but are not limited to, computers, tablets, phones (smartphones, Voice Over IP phones, land lines), data communication equipment, network equipment, software, voice mail, Instant Messaging, text messaging, documents, spreadsheets, calendar entries, appointments, tasks, and notes which reside in part or in whole on any City electronic system or equipment.

An employee's communications and use of electronic systems will be held to the same standard as all other business communications, including compliance with the City's discrimination and harassment policies. Employees are expected to use good judgment in their use of any electronic systems as defined above. Employees should notify their Supervisor, Manager, Director, the Personnel Services Department (PSD) or the Information Services Department (ISD), or follow their department specific policy, if any, to notify the appropriate person of any unsolicited, offensive materials received by any employee on any electronic system.

The City has the authority to inspect any City owned systems, including but not limited to, computers, smartphones, email, files and other electronic tools, and GPS in the normal

course of business at any time. Departmental requests for such information shall be in the form of a request to ISD to extract information, files, documents, voice mail, instant messages, or any other form of information maintained through the City owned systems, through authorization by the City Manager, City Attorney, Chief Information Officer, or designee. Reasons for review include, but are not limited to, system hardware or software problems, security issues, general system failure, a legal action taken against the City, public records requests, suspected unlawful activity or violation of policy, or a need to perform work and/or provide a service when the employee is unavailable. ISD shall have the ability to inspect devices as a course of normal business for the purpose of troubleshooting, security issues, cyber threats, configuration issues, the identification of unauthorized software, misuse, and other appropriate business reasons. Any inspections outside of the normal course of business will be through authorization by the City Manager, City Attorney, Chief Information Officer, or designee.

Confidential Data/Privacy

The City shall put in place reasonable provisions to protect confidential personal data, however, employees who use electronic systems and/or tools provided by the City cannot be guaranteed absolute privacy. Any and all opinions, statements, images, communications, or other transmission of information made using these systems, whether implied or expressed, are those of the individual and not necessarily of the City or management.

Employees who communicate or share information through the use of the City's electronic systems with the City Attorney's Office related to any legal advice or legal issue shall not share any attorney-client privileged communications or information with anyone not expressly authorized to receive that confidential communication or information, without the express approval of the City Attorney's Office.

Uses of Electronic Systems and Information

Electronic systems, hardware, software, tools and information are provided for the purpose of conducting business for the City.

A. Allowable uses of electronic systems and information include the following, to the extent that these uses are for the purpose of conducting City business:

    1. To facilitate performance of job functions.
    2. To facilitate the communication of information in a timely manner.
    3. To coordinate meetings of individuals, locations, and City resources.
    4. To communicate with departments throughout the City.
    5. To communicate with outside organizations as required, in order to perform an employee's job functions.

B. Prohibited uses of electronic systems and information include, but are not limited to the following:

1. Illegal activities
2. Threats
3. Harassment
4. Slander
5. Defamation
6. Obscene or suggestive messages or offensive graphical images, including but not limited to, pornographic images or other content, violent images or other content, or anything a reasonable person would find offensive, including any messages, images or content that may violate Administrative Order 2-16.
7. Political endorsements or solicitations
8. Commercial activities
9. Using non-business software including games, unauthorized mobile apps, third party screen savers, search engine toolbars or other web browser add-ons, unapproved backgrounds or entertainment software.

C. Unauthorized uses of electronic systems and information include, but are not limited to, the following:

1. Using hardware or related computer equipment and software not purchased and/or owned by the City.
2. Revealing your account password to others or allowing the use of your account by others.
3. Listening to voice mail or reading electronic mail of another employee without prior written approval of the employee's Department Head or executive management. An employee's supervisor may inspect the contents of voice mail or electronic mail pursuant to the section titled "*Ownership*" of this policy.
4. Using a City system or software to conduct non-City business (beyond incidental personal use, as set forth within this policy).
5. Sending confidential information to unauthorized recipients.
6. Storage of copyrighted multimedia files (including music and videos) on City computers, tablets, cell phones or servers.
7. Perform unauthorized or illegal actions, such as hacking, fraud, or buying/selling illegal goods.
8. Instant messaging over the internet is not permitted using a non-City approved system. Use of enterprise-wide instant messaging (Microsoft Lync) is acceptable for work purposes.
9. Non-work related streaming media (audio or video) on desktops, laptops, or tablets. Examples include television broadcasts or replays, radio, sports, music or news stations, personal videos, YouTube, Google Video, FaceBook or other similar media.

D. Personal Use:

Incidental personal use is acceptable unless it interferes with daily work and violates any stipulations within this policy. Incidental personal use should be considered in the same context as incidental phone usage. In addition, the City's systems are not intended to be used for personal storage and the City is not responsible for the retrieval and/or loss of any personal storage that may have been placed on a City system. Any personal use of the City's electronic systems beyond incidental personal use, to be determined on a case-by-case basis, could subject the employee to disciplinary action, up to and including termination.

E. Tampering:

In no way shall an employee intentionally tamper, deface or damage City electronic equipment. This includes the removal of software or changing the configuration of a device without proper authorization from the Information Services Department.

Passwords

It is the responsibility of each employee to remember and safeguard their system passwords. Personal account passwords are not to be shared. The Information Services Department may require verification of identification before using a new password in the event that a password is forgotten or cease to function.

Workstation Hardware and Software

In order to ensure that workstations citywide can be maintained in a timely and cost effective manner, and to ensure that the City is compliant with software licensing, the following guidelines and restrictions apply:

A. All software installed on City workstations must be legally licensed by the City.
B. Employees are not authorized to install personal copies of software on City workstations.
C. All hardware, software installations and upgrades on City workstations must be performed by authorized personnel. Employees are not authorized to install or upgrade workstation hardware or software.
D. Information Services is authorized to run software on each workstation to provide necessary support and inventory services.
E. To ensure compatibility and interoperability between all City workstations, workstation software must adhere to standards made available by Information Services. These standards will apply to operating systems, email systems, office suite software and internet browsers. Information Services will grant exceptions to standards on a case-by-case basis as required to perform valid business functions.
F. Employees shall not use hardware boot passwords.

Cell Phones/Smartphones other Cellular Data Devices

The City may issue a cellular telephone, smartphone, or pager if deemed appropriate for an employee's job responsibilities. Devices/services are approved by the employee's Department Director, Assistant Director or Manager, on the basis of need. Each department is responsible for the determination of the need as well as the usage.

Cell phones/smartphones and other cellular device use shall follow the same stipulations as any other electronic tool. In addition, employees are responsible for following appropriate California Vehicle Codes when operating such a device in a vehicle:

> Vehicle Code (VC) §23123 states it is illegal to operate a wireless telephone without a "hands-free" device while operating a motor vehicle, with the exception of emergency services (includes Fire, Police and Health Care operations). Vehicle Code (VC) §23123.5 also prohibits any action to "write, send, or read a text-based communication" which includes email and instant messaging.

Any employee found in violation of the "hands free" law will be responsible for citations received, and possible disciplinary action. It is the employee's responsibility to review Vehicle Code (VC) §23123 and §23123.5 to be aware of all restrictions, exemptions and violation fines.

Employees should exercise great care in the protection of the data of the phone by at least implementing a screen lock or password. In addition, if the phone is lost or stolen, ISD should be contacted as soon as possible.

Procedures

This policy will be provided to all employees and an acknowledgement shall be signed.

Employee Responsibility

Effective security involves the participation and support of every City employee and affiliate who deals with electronic information systems. Each employee with access to City electronic systems and tools is responsible for understanding and following these guidelines and to conduct their activities accordingly. Unauthorized or improper use of the City's electronic systems and tools may result in terminating access. Additionally, City employees, depending on the nature, extent, and/or consequences of any unauthorized or improper use of the City's electronic systems, may be subject to disciplinary action, up to and including termination.