
Information Technology Use

704.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of District information technology resources, including computers, electronic devices, hardware, software and systems.

704.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), hardware, software, and resources owned, leased, rented or licensed by the Fresno County Fire Protection District that are provided for official use by members. This shall include all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the District.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones including cellular and satellite, pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs, systems and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file or file - Any electronic document, information or data residing or located, in whole or in part, on the system, including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports or messages, photographs or videos.

704.2 POLICY

Fresno County Fire Protection District members shall use information technology resources, including computers, software and systems, that are issued or maintained by the District in a professional manner and in accordance with this policy.

704.3 PRIVACY EXPECTATION

District Members forfeit any expectation of privacy with regard to emails, texts or anything published, shared, transmitted or maintained through file-sharing software or any Internet site that is accessed, transmitted, received or reviewed on any technology system.

The District reserves the right to access, audit and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received or reviewed over any technology that is issued or maintained by the District, including the District email system, computer network or any information placed into storage on any District system or device. This includes records of all keystrokes or Web-browsing history made at any District computer or over any District network. The fact that access to a database, service or website requires a username or password will not create an expectation of privacy if it is accessed through District computers, electronic devices or networks.

Information Technology Use

However, the District may not require a member to disclose a personal username or password or open a personal social website, except when access is reasonably believed to be relevant to the investigation of allegations of work-related misconduct (Labor Code § 980).

704.3 RESTRICTED USE

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to their supervisor or Fire Chief.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

704.3.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes, in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software infection, members shall not install any unlicensed or unauthorized software on any District computer. Members shall not install personal copies of any software on any District computer. Any files or software that a member finds necessary to install on District computers or networks shall be installed only with the approval of District information systems technology (IT) staff and only after being properly scanned for malicious attachments.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the District while on District premises, computer systems or electronic devices. Such unauthorized use of software exposes the District and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as a part of the automated maintenance or update process of District-approved or installed programs by the original manufacturer, producer or developer of the software. Any other introduction of software requires prior authorization from IT staff.

704.3.2 HARDWARE

Access to technology resources provided by or through the District shall be strictly limited to District-related activities. Data stored on or available through District computer systems shall only be accessed by authorized members who are engaged in an approved District-related project or program or who otherwise have a legitimate District-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

704.3.3 INTERNET USE

Internet access provided by or through the District shall be strictly limited to District-related activities. Internet sites containing information that is not appropriate or applicable to District

Information Technology Use

use and which shall not be intentionally accessed include, but are not limited to, adult forums, pornography, gambling, chat rooms, and similar or related Internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member's assignment.

Downloaded information from the Internet shall be limited to messages, mail and data files.

704.3.4 OFF-DUTY USE

Members shall only use technological resources related to their job while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor.

704.3 INSPECTION OR REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the District involving one of its members or a member's duties, an alleged or suspected violation of any District policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the District computer system when requested by a supervisor or during the course of regular duties that require such information.

704.3 PROTECTION OF SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care and maintenance of the computer system.

Members shall ensure District computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information and other individual security data, protocols and procedures are confidential information and are not to be shared. Password length, format, structure and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the Internet) to a supervisor.