STANISLAUS CONSOLIDATED FIRE PROTECTION DISTRICT
POLICIES & PROCEDURES

ARTICLE: C-22
SECTION: Operations Division
DATE: 10/18/1999
SUPERSEDES:
TITLE: **ELECTRONIC MEDIA USE**

SECTION 1: PURPOSE:

This policy addresses the use of Electronic media by all SCFPD employees. For the purpose of this policy employees shall mean all full time, part time or volunteer personnel.

SECTION 2: DEFINITION

This policy applies to Electronic Media, and all documents, recordings and other data contained in or recoverable from such media used within the District.

A. Electronic Media. Electronic Media includes all types of electronic equipment, such as telephones, computers, computer peripherals, photocopy machines, fax machines, computer software, laptops, voice mail, electronic mail (e-mail), Internet access, World Wide Web access, online information service, and any other electronic type of equipment that the District deems as Electronic Media.

B. Information. Information consists of any kind of information used in any way with the Electronic Media. Examples include messages, communications, e -mails, files, records, recordings, images, graphics, transmissions, signals, programs, software and any other data.

C. Use. Use is the operation or application of Electronic Media to affect information in any way. Examples include using Electronic Media to search, produce, calculate, forward, print, publish, receive, recover, send, transmit, apply, run, control, download, upload, record, copy, rename, access, alter, delete, erase or store any information.

D. District and Personal Equipment. This policy applies to all Electronic Media provided by the District, as well as Electronic Media used on District property for District business purposes.

SECTION 3: POLICY

Stanislaus Consolidated Fire Protection District supports the use of technology to improve customer service, promote public participation in local government, increase staff productivity, reduce operating costs and facilitate collaborative government-related work.

Universal service and access technology for all residents are a priority for SCFPD. The District encourages employee use of Electronic Media when it enhances service, work productivity, research capabilities and other benefits to the District.

Electronic Media are provided for the use of District employees for District business-related purposes. As with all District resources, Electronic Media are provided for District business only, and should not be used for any extraneous commercial, political, or religious purposes unless otherwise specifically authorized by the Fire Chief.

SECTION 4: USE OF ELECTRONIC MEDIA

A. Privacy. Employees have the right to know that information they use is not confidential or private. All of the District's Electronic Media and information relating to these Electronic Media are District property. Although employees have passwords that restrict access to their computers, the District reserves the right to access this information. While Electronic Media files and information will no be monitored as a routine matter, the District reserves the right to do so without prior notification. By way of example, the District may electronically scan mail messages for the presence of specific content such as viruses or passwords and to maintain system integrity. The District will also respond to legal processes and fulfill any obligation to third parties.

Only Duty Chiefs or higher can authorize the reading of e-mail for employees under their supervision. Unauthorized monitoring or reading of the District's e-mail systems or their contents violates the District policy and may result in disciplinary action.

It should be noted that even though information or files may have been deleted from Electronic Media, it does not mean they have been permanently erased from the system. It is possible to recover deleted computer files and deleted e-mail.

In addition to the foregoing provisions, employees should be aware that certain kinds of Electronic Media Information may be subject to record retention requirements or disclosure, either as "public records" or pursuant to discovery in litigation.

B. E-mail. The District's policy on privacy and Electronic media applies to e-mail. E-mail is a fast and convenient way to communicate. Its use should be encouraged throughout the District. The ease in which e-mail facilitates communication can often lead to problems: the recipient of a message can forward it to any number of individuals and messages may accidentally be delivered to the wrong recipient. The possibility of such events necessitates that employees exercise care when composing and sending e-mail messages.

C. Online Information Service use. Periods of access to online information services such as Internet and the World Wide Wed should be kept to a reasonable amount of time, as determined by the Fire Chief. As with all District resources, online access is provided for District business only, and should not be used for any extraneous commercial, political, or religious purposes unless otherwise specifically authorized by a Fire Chief.

D. Software installation. With a shared wide-area network (WAN), the installation of software on one part of the WAN has the potential to affect other users on the WAN. Computer viruses are of particular concern. Additionally, the law requires that all software residing on any District computer must be licensed, and reduce the potential of introducing a computer virus, employees must receive approval from the Fire Chief before adding software programs to District computers. Failure to secure this written approval will result in disciplinary action.

E. Copyright Protection. Under most circumstances, it is illegal to reproduce or distribute copyrighted information without permission for the copyright owner. These copyright laws are applicable to much of the information available over the Internet. The District and its employees are required to abide by the federal copyright laws and to abide by all licensing agreements.

SECTION 5: APPROPRIATE USES OF ELECTRONIC MEDIA

Appropriate use of Electronic Media for District business purposes include, but are not limited to, the following:

- to perform tasks assigned by a supervisor;
- to enhance performance of job functions;
- to facilitate communication of information within the District;
- to coordinate meetings of individuals, locations and resources of the District;
- to communicate with outside organizations as required in order to perform an employees job function;
- to provide educational opportunities during non-business hours and with prior approval from the Fire Chief.

SECTION 6: UNACCEPTABLE USES OF ELECTRONIC MEDIA

Prohibited uses of Electronic Media include, but are not limited to the following:

- Activities illegal under local, state and/or federal law;
- Anything that may be constructed as harassment or disparagement of others based on the guidelines established in the District's Discrimination Policy and Sexual Harassment Policy (see Discrimination or Sexual Harassment Policy for description);
- Fund raising, soliciting or other religious or commercial activities that are not specifically related to District activities;
- Sabotage (e.g. intentionally disrupting network traffic, crashing the network, intentionally introducing a computer virus, etc.);
- Unauthorized access to others' files or vandalizing the data of another user;
- Forging electronic mail messages or any other form of communication;
- Personal messages such as chain letters; and
- Inappropriate use, which is deemed by the District to be a violation of the intended use of any of the Electronic Media.

SECTION 7: VIOLATIONS POLICY

Violation of this policy will be reviewed on a case-by-case basis and may result in disciplinary action, up to and including discharge.

Written By: Dan Reeves Date: October 18, 1999