Scotts Valley Fire Protection District	
POLICY: 2201	**SUBJECT:** Computer Management
DATE APPROVED: 7/14/2021	
BOARD PRESIDENT:	**FIRE CHIEF:**

PURPOSE:

This policy provides the guidelines for the use of Scotts Valley Fire Protection District (SVFPD) computers by SVFPD personnel and Board Members. It specifically governs the use of the SVFPD computer system for emails, files, data, software, images, voice mails, text messages, electronic communications, and stored electronic communications. This policy clarifies employee expectation of privacy as it relates to the workplace use of computers, emails, files, data, software, images, voice mails, text messages, electronic communications, and stored electronic communications. This policy shall fully apply to SVFPD issued cellular telephones, personally owned cellular telephones, personally owned computers, and other SVFPD issued or personally owned electronic devices that utilize the SVFPD computer system for access to the intranet and/or Internet.

DEFINITIONS:

Electronic device – a computer, cellular telephone, smartphones, personal data assistant (PDA), pager, two-way paging device, iPad, iPod, Kindle, or similar device capable of sending and receiving an electronic communication.

Electronic Communication: Any transfer of signs, signals, writings, images, sounds, data or intelligence that is created, sent, forwarded, replied to, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, printed, or otherwise transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system. This term expressly includes, but is not limited to, emails, attachments to emails, text messages, instant messages, recorded voicemail messages, web sites visited, computer files, data files, and live or recorded streaming video or audio sent over the intranet or Internet, or sent by wired or wireless communication.

Stored electronic communication: Any temporary or intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; any storage of an electronic communication for purposes of backup protection of such communication; and any other storage, retention, backup, or archiving of an electronic communication, whether accident, incidental or purposeful, utilizing an electronic storage medium.

Internet: The world-wide system of interconnected computer networks that consists of millions of private, public, academic, business, and government networks linked by a broad array of electronic and optical networking technologies.

Intranet: The SVFPD's internal computer system and network

PROCEDURE:

I. General:

1. The SVFPD computer system, including all SVFPD issued computers, laptops, notebooks, tablets, electronic devices, hardware, the intranet, and access to the Internet provided by the SVFPD, are owned by the SVFPD. The use of such systems, equipment and access is conditioned upon employee consent to the terms of this policy.

2. The SVFPD computer system, SVFPD computers and hardware, the intranet, and access to the Internet provided by the SVFPD, may not be used by employees for personal gain, including personal businesses, but rather is available to enhance the service that the SVFPD provides to the public.

3. The SVFPD reserves the right to examine, monitor, intercept, review, copy, store, save, and forward to third parties any and all electronic communications sent or received over the SVFPD computer system, as well as any stored electronic communication or other files stored on a SVFPD computer, hard drive, memory device, or storage medium. The failure of the SVFPD to exercise its rights under this section, shall not constitute a waiver of these rights.

4. Employees are advised that they have no expectation of privacy in any electronic communication, stored electronic communication, file, image, sound, message, website visited, or other action or activity while working on a SVFPD computer, or while using any other computer, cellular telephone, or electronic device that is accessing the SVFPD computer system, including while accessing the Internet through the SVFPD computer system.

5. Employees are advised that they have no expectation of privacy in any electronic communication, stored electronic communication, file, image, sound, or message contained on a portable memory device such as a hard disk, flash drive, memory card, CD-ROM, DVD, or other media that is attached to/accessible by a SVFPD computer, or is attached to/accessible by an electronic device that is accessing the SVFPD computer system.

6. Employees are responsible for any information that they view, access, generate or distribute through the SVFPD computer system.

7. Employees are required to prevent the unauthorized use of the SVFPD computer system, and shall use password–protected screen savers or other appropriate techniques while away from their computer. Any use that occurs on an employee's workstation under that employee's login is presumed to be performed by that employee. Employees must log off the computer when not using it, and before leaving the computer unattended.

II. Email

1. Only SVFPD personnel and Board Members are allowed access to the SVFPD e-mail system.

2. Employees and Board Members should not use their SVFPD e-mail account as their primary personal e-mail address.

3. Incidental or occasional use of SVFPD e-mail for personal reasons is permitted.

4. The following e-mail activity is prohibited:
    a. Accessing, or trying to access, another user's e-mail account without authorization

b. Obtaining, or distributing, another user's e-mail account
c. Using e-mail to harass, discriminate, or make defamatory comments
d. Transmitting SVFPD records within, or outside, the SVFPD without authorization
e. Advertising political activities which benefit one political candidate or party
f. Advertising purely commercial activities or events
g. Any activities which are inconsistent with the mission of the SVFPD
h. Any illegal activities

5. Employees and Board Members are reminded that email messages may be subject to public disclosure under the Freedom of Information act, and may be discoverable during litigation. Assume any email sent over the SVFPD system will be viewed by the public.

III. Confidentiality

SVFPD personnel routinely handle information that is considered to be confidential under federal and state law. This includes information relative to incidents, investigations, patients, and employees, and may include confidential personal information, financial information, and medical information. The following conduct is prohibited when dealing with confidential information:

1. Forwarding or sending confidential information to someone not authorized by law to receive it.

2. Printing confidential information to a printer in an unsecured area and leaving the documents unattended.

3. Leaving a computer unattended with confidential files logged on, accessible, or visible.

4. Leaving memory media with confidential data unattended, in easy to access places.

IV. Prohibited Activities

The following uses of the SVFPD computer system are prohibited:

1. Personal use of the SVFPD computer system that interrupts SVFPD business and that keeps an employee from performing their work.

2. Extensive personal use of the Internet for non-work-related purposes during working hours which decreases employee productivity.

3. Unauthorized downloading and/or distributing of copyrighted materials (e.g. music, videos, photos, games, software, or other proprietary information).

4. Downloading or copying music, videos, photos, or games for non-business purposes onto SVFPD computers or servers.

5. Unauthorized reading, deleting, copying, modifying, or printing of electronic communication of another user.

6. Using the SVFPD computer system for private gain or profit, including but not limited to, online gambling, personal business, on-line auctions (e-Bay), stock trading, etc.

7. Soliciting or using SVFPD computers for political, religious or other non-SVFPD reasons.

8. Using, viewing, accessing, or transmitting pornographic or sexually explicit materials, or materials that are offensive, threatening, or constitute hate mail/messaging pertaining to race, national origin, gender or religion.

9. Engaging in any form of harassment, whether sexual or otherwise, or sending any unwelcome personal communication after being asked or instructed to cease communications. It is the perception of the recipient that prevails, not the intention of the sender.

10. Breach or attempt to breach any security mechanisms, hack-into, defeat, disable, or otherwise manipulate the intranet or SVFPD computer system in order to circumvent a technological measure to gain access to information in ways not permitted or authorized, or to cause the system to react or respond in ways other than as intended by the SVFPD administration.

11. Engaging in any illegal activity.

POL 2201 – Form 1