SCOTTS VALLEY WATER DISTRICT
svwd.org svwater

Policy

Number:	P100-17-3	**Type of Policy:**	Administration
Title:	Technology Resources		
Description:	Establishes standards and guidelines for access and use of District Technology Resources.		
Original Adoption	05/04/17	**Reviewed:**	04/13/23
Review Cycle	4 years	**Resolution No.:**	03-19

The Scotts Valley Water District (District) recognizes that access to electronic technology and communications networks, including internet and emails, is an integral part of its business function. Many tasks performed in the normal course of business require that employees use the District's electronic technology resources and communications networks. There is not always a clear delineation between work and personal life when it comes to technology.

This policy establishes standards that protect the District and its employees, and outlines acceptable use of technology resources, taking into consideration legal responsibilities, employee privacy concerns, as well as operational needs. Compliance with this policy is essential, and violation of any aspect may result in disciplinary action up to, and including, termination.

Covered Technology

This policy extends to all features of the District information technology, communications network, and systems, including, but not limited to, computers, file servers, email, connections to the Internet and other external networks, telephones, mobile devices, smart phones, video conferencing, text messaging, including both District provided devices and personal devices used for District business. All other forms of electronic communication used by employees currently or in the future are covered.

District Provided Devices

The following rules have been established for use of the District's technology and communications networks, including the Internet and email:

1. All technology provided by the District including computer systems, communications networks, District-related work records and other information stored electronically, is the property of the District. In general, use of the District's technology systems and electronic communications should be job-related and not for personal convenience.
2. Employees may not use the District's Internet, email or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's

race, age, disability, religion, national origin, physical attributes or sexual preference may be transmitted. Harassment of any kind is prohibited.

3. Disparaging, abusive, profane or offensive language; materials that might adversely or negatively reflect on the District or be contrary to its legitimate business interests; and any illegal activities including piracy, software cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet or email are forbidden.
4. Copyrighted materials belonging to entities other than the District may not be transmitted by employees on the District's network without permission of the copyright holder. Employees must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy for reference only. Saving copyright-protected information to a network drive without permission is prohibited. Sharing the URL (uniform resource locator or "address") of an internet site with other interested persons for business reasons is permitted.
5. Employees may not use the system in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and "spamming" (sending email to thousands of users.)
6. To prevent contamination of the District technology and communications equipment and systems by harmful malware and computer viruses, employees should only open email attachments from senders that they know or are expecting the email attachment. Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files. Malware and computer viruses can be spread through downloads from the internet. Files from unknown sources should not be downloaded.
7. Employees are responsible for the content of all text, audio or image files sent over the District's Internet and email systems. No email or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else.
8. Email and other electronic communications transmitted by the District equipment, systems and networks are not private or confidential, and are the property of the District. The District reserves the right to examine, monitor and regulate email and other electronic communications, directories, files and all other content, including Internet use, transmitted by or stored in its technology systems, whether onsite or offsite.
9. Internal and external email, voice mail, and text messages are considered business records and may be subject to discovery in the event of litigation. Employees must be aware of this possibility when communicating electronically within and outside the District.

Security

An important security feature that protects District electronic data communication is the use of passwords. Employee passwords are used for security purposes and do not affect District ownership of the electronic information. Passwords are intended to protect information from those that do not have access to such information. All passwords created by or issued to the user should not be shared, given, or otherwise disclosed to any other person.

District employees will:

1. Take every effort to protect District issued devices from theft, damage, abuse and unauthorized use.
2. Immediately report if a device is stolen, lost or damaged.
3. Take appropriate measures to safeguard District data when using district or personal mobile devices.
4. Not download any software or applications without prior authorization.

Software Usage

The District purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, District does not have the right to reproduce such software for use on more than one computer. As such, employees may only use software on local area networks or on multiple machines according to the software license agreement. The District prohibits the illegal duplication of software and its related documentation.

Access of Another Person's Electronic Communications

Employees may not intercept, record, read, alter, retrieve, receive, send, or use another employee's electronic identity unless designated by management to serve as a proxy, as discussed below.

Email Retention

The District retains emails on the server for a period of time. The content of some email messages could be classified as a record pursuant to the guidelines established by management consistent with the District's Records Retention Policy

E-Signatures

The District uses DocuSign for electronic-signatures. Documents are encrypted and an audit trail is maintained.

Internet Usage

Internet access is provided to employees for the benefit of the District. Employees represent the District and are responsible for Internet use in an effective, ethical, and lawful manner. Each employee is responsible for the content of all text, audio, or images that they place or send over the Internet. Fraudulent, harassing, or obscene messages are prohibited. All messages communicated over the Internet should have your name attached, unless authorized as a proxy. No messages should be transmitted under an assumed name.

Telephones/Mobile Devices

The District telephone system comprises of a desk phone, soft phone and a mobile device. District telephones may be used for necessary personal calls; however, employees are not to use them to call 1-900 or directory assistance calls.

Personal Use of District Mobile Devices

The District provides electronic communications devices (e.g., cell phones, iPads, laptops) to its employees, based on an identified need of conducting business. They are subject to the following:

- Employees should ensure that personal use of these items does not interfere with District business or

the productivity (personal use should take place during breaks and/or lunch).

- Personal use may not involve any prohibited activity described in this Policy.
- Personal use may not disrupt or delay the performance of District business.
- Personal use must not be for personal gain or commercial ventures.
- Personal use may not support or advocate non-District related business purposes.
- Incidental personal data (such as personal calendars, personal address lists, and similar incidental personal data) may be prepared and stored in a reasonable manner, provided such use does not conflict with any purpose or need of the District.
- Necessary personal communications may be sent and received through email, as long as such activity does not interfere with productivity or jeopardize the security of District data or systems.

Remote Access to the District Network and Related Systems

Remote access to the District's network servers or web-based applications, whether through a virtual network or other means will be authorized by the General Manager.

- All rules that apply to the working of overtime and the consequences of working unauthorized overtime apply in the context of working remotely.
- Non-exempt employees should not access the network outside of regularly scheduled work hours, unless such remote access meets a legitimate business need and has been previously approved by the employee's immediate supervisor.
- Employees will not download or transfer sensitive business data to their personal devices, which is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), proprietary information, or District financial operations.
- Personal devices used to access the District network remotely must be password protected and appropriate measures to safeguard District data must be taken.
- Employees must delete any sensitive business files that may be inadvertently downloaded and stored on a personal device through the process of viewing email attachments.

Mobile Device Stipend Plan

Employees using their personal mobile device to conduct District business will receive a mobile device stipend.

Employees utilizing their personal mobile devices will be responsible for costs, maintenance and support of their personal mobile device.

The District cannot and does not imply, extend, or guarantee any right to privacy for work-related voice calls and/or electronic communications placed. The District does not remotely monitor or remotely access any information contained on the employee's personally owned mobile device. However, employees

acknowledge that all District work products generated or stored on any personally owned device is potentially subject to disclosure through subpoena or other legal recourse. The employee acknowledges that any such request could require them to search their personal device and disclose any and all District work products, including but not limited to, call detail records, logs, voice mail messages, data storage, text messages, emails, and address books when utilized for the purpose of conducting District business.

District Website

The svwd.org website represents a fundamental communication tool for providing information and is for official use only. The District maintains responsibility for website content and postings.

Social Networking

The District uses social networks such as Facebook and NextDoor as forms of public communication. The General Manager or his/her authorized designee may post District related material to social media sites.

Employees have an obligation to ensure that any public electronic communication they make, including social networking communications, does not negatively impact the reputation of District. Engaging in social networking during the workday can negatively impact productivity and work performance. It is the employee's responsibility to regulate their social networking so that it does not impact productivity or cause performance issues.