Sacramento Suburban Water District

Technology Use Policy

Adopted: September 20, 2004
Approved with Changes: May 20, 2024

100.00 Purpose of the Policy

The purpose of this policy is to provide guidelines for the appropriate use of all technology resources provided by the District. These resources include computers, servers, printers, scanners, software, Internet, Intranet, phones, copier/fax machines, and all other technology-related devices and data.

200.00 Policy

The District uses various forms of electronic communication and equipment including, but not limited to computers, tablets, printers, modems, telephones, cell phones, voice mail, copier/fax machines, internet, texting, and e-mail (collectively referred to as "electronic facilities"). All electronic facilities and data are and will remain the sole property of the District. All messages sent and received, including any personal messages, and all data and information stored on the District's electronic facilities are the District's property regardless of content.

200.10 Social Media

Use of District electronic facilities to access and use any form of social media for personal purposes is not permitted. Employees who may need to use social media for District-related business must obtain prior approval from the General Manager or his/her designee and comply with the District's Social Media Procedures promulgated by the General Manager. Any form of social media used by the District as an outreach or communications tool are subject to the Social Media Procedures promulgated by the General Manager and shall not be used in a manner that creates an open public forum.

200.20 Specifically Prohibited Usage/Activity

Electronic facilities will not be used in any manner that would: (1) be discriminatory, lewd, derogatory, defamatory, disparaging, sexually explicit, harassing, threatening, or obscene; (2) constitute copyright, trademark infringement or misappropriation of trade secrets; or (3) be for any other purpose which is illegal, against District policy, or not in the best interests of the District.

Unless pre-approved by the Information Technology Manager or the General Manager, the use of personal software or peripheral devices installed on or connected to District electronic facilities is not authorized, including, but not limited to:

1. A piece of software acquired for one's home computer
2. Downloaded software from the internet
3. Any proprietary software or data not licensed to the District
4. Personal flash drives or other portable storage devices

External connections to the District's internal network are not permitted unless expressly authorized in advance by the Information Technology Manager or the General Manager and necessary for a District purpose.

Employees must not place stickers, decals, tape or other such attachments on District electronic facilities unless expressly authorized.

200.30 Software Installation and Usage

To avoid any security breach or other harm, employees will not install personal software in District electronic facilities. Unless otherwise determined by the Information Technology Manager or other qualified person, all software on the Internet should be considered copyrighted work. Therefore, employees are prohibited from downloading software and/or modifying any such files without permission from the copyright holder.

All software on any District electronic facility must be licensed to the District. Any updates to existing software must be approved by the Information Technology Manager prior to installing the update.

200.40 Ownership and Privacy

All electronic information created by any employee using any District facility is the property of the District and will remain the property of the District. **Employees should understand that they have no right or expectation of privacy with respect to any messages or information created or maintained on the District's electronic facilities, including personal information or messages, and that any electronic information created, sent, received or accessed by an employee may be a public record subject to disclosure upon request.** Personal passwords may be used for purposes of security, but the use of a personal password does not affect the District's ownership of, or ability to access, the electronic information.

All District electronic facilities provided to employees for the performance of District work will remain the property of the District. Employees are expected to exercise due care and proper safeguards while using District-provided electronic facilities and to notify the Information Technology department in the event of any potential or actual damage, breach, theft or other loss of District electronic facilities or data immediately.

The District reserves the right to enter, access, search, monitor, review, copy, and/or retrieve electronic files, messages, e-mail, texts, voice mail, history of internet usage, and any other type of electronic file or information created or stored on any District electronic facility, without notice, for any legitimate business purpose including, but not limited to, ensuring that there is no misuse or violation of District policy or any law, investigating theft, and monitoring disclosure of District information. The District may override personal passwords if it becomes necessary or appropriate to do so for any reason.

200.50 Data Management and Protection

All employees must use, manage and protect District records resulting from their use of District electronic facilities as required by this policy, the District's Records Management Policy (PL - Adm 002), Electronic Communications System Management and Retention Policy (PL - IT 003) and all related procedures promulgated by the General Manager, which set forth the responsibilities of all District employees concerning the creation, storage, protection, retention, and disposal of electronic documents and communications that are designated as either official or not official District records. Employees are advised that if they use their personal electronic devices on District business, they may be creating District records that must be preserved and that may subject their personal electronic devices to surrender to the District to search for, view, and possibly extract any District records.

Drafts, copies, duplicates, support files and other types of documents as outlined in Policy PL – Adm 002 Records Management Policy, Section 300.30.b should be removed from District electronic facilities (especially file stores and email) when no longer required. The email system is not to be used as a file storage system. Attachments should be removed and stored with other electronic files in appropriately designated locations in accordance with District Policy PL – IT 003 Electronic Communications System Management and Retention Policy, Section 100.10 and 200.00.

The Internet does not guarantee the privacy and confidentiality of information. Sensitive District records or other material transferred over the Internet may be at risk of detection or interception by a third party. Employees must exercise caution and due care when transferring such records and materials over the internet. When possible, Employees should use a file sharing site or other secure program for transmitting files instead of attaching sensitive information to an email.

The use of internet based AI (Artificial Intelligence) platforms to assist with content creation should never include any Personal Identifiable Information (PII) of customers or District staff.

The introduction of viruses, malware or malicious tampering with any electronic facility is expressly prohibited. Employees are to use extreme care when opening links

or attachments to ensure they are free from viruses or malicious code that could infect District electronic facilities. Files that are downloaded from the internet must be checked with virus detection software before being opened and used. The truth or accuracy of information on the internet and in unsolicited e-mails should be considered suspect until confirmed by a separate (reliable) source.

200.60 Policy Violation

Any employee who misuses the District's electronic facilities or otherwise violates this policy or its related procedures will be subject to discipline up to and including termination.

300.00 Policy Review

This policy shall be periodically reviewed by the Board of Directors in accordance with its established policy review schedule.