Vallecitos Water District

INTERNET AND ELECTRONIC COMMUNCATION SYSTEMS POLICY

Introduction

This policy was established to ensure all employees utilize the District's computers, mobile devices, internet, and electronic communication systems, in a legal, ethical, and appropriate manner. The overriding goal of this policy is to secure and protect the integrity of data that resides within the District's technology infrastructure, and prevent this data from being accessed and deliberately or inadvertently stored, transferred or carried on an unsecured computer, mobile device or over an unsecured network.

Policy

All devices connected to a District managed or unmanaged network, used to backup, store, or otherwise access District data of any type must comply with this policy. This includes devices outside of the District's direct control, such as personal mobile devices. Prior to initial use on the District network or related infrastructure, all devices must be registered with the District's Information Technology (IT) Department.

All employees of the District are subject to this policy and expected to read, understand, and comply fully with its provisions. There is no expectation of privacy with electronic communications. Personal use is allowed but must be kept to a minimum. Any unlawful, unethical, or inappropriate use of the District's internet and electronic communication systems is strictly prohibited and may be grounds for discipline.

Definitions

Devices: Desktop, home, or personal computers (PCs), laptops, notebooks, tablets/iPad's, cellular phones, used to access District resources, and any mobile device capable of storing District data and connecting to an unmanaged network.

Electronic Communication: All forms of the District's electronic communication systems and equipment used currently or in the future, including computers, e-mail, connections to the internet and other networks, voice mail, facsimiles, and telephones.

User: Anyone who uses the District's internet and electronic communications systems.

User Responsibilities

- Use reasonable physical security measures with all mobile devices.
- Password-protect all devices; do not leave passwords unsecured or share them.
- Install up-to-date anti-virus and anti-malware software on any non-District devices used to connect to the District's network.
- Do not modify District software or install applications without permission.

User Responsibilities (continued)

- Immediately report any unauthorized data access, data loss, and/or disclosure of District resources, databases, networks, etc.
- Immediately report any lost or stolen devices.
- Permanently erase all District related email, data and files from devices when no longer needed and/or after required retention period.
- Be aware of the possibility of emails being used for litigation or public records.
- Delete messages received that were intended for others and inform the sender.
- Keep personal use to a minimum.
- See full list of prohibited activities including, but not limited to, streaming, chain letters/emails, and gambling.

No Expectation of Privacy

No user should have any expectation of privacy with respect to information transmitted, received, or stored in any electronic communications systems or equipment owned, leased, or operated in whole or in part by, or on behalf of, the District. The District has a right to monitor all aspects of their computer systems and equipment usage, such monitoring may occur at any time, without notice, and without the user's permission.

Limited Personal Use

Personal use is any use that is not job related. Access to the internet through the District's network is a privilege and carries responsibilities reflecting responsible and ethical use. Employees may use the District's electronic communications system for personal use provided personal use is limited and kept to a minimum. Personal use cannot interfere with the user's productivity or work performance, or with any other employee's productivity or work performance. Actions cannot be illegal, unethical, inappropriate, or in violation of any District policies. In additional, personal use cannot adversely affect the efficient operation of the electronic communication systems.

Social Networking

All employees have an obligation to the District to ensure that any public communication, including social networking communications, do not negatively impact the District, its partners, customers, suppliers, etc. Only a select group of employees are authorized to publicly speak on behalf of the District. In addition, it is the employee's responsibility to regulate social networking to comply with this policy, including limited personal use. Employees are responsible for communications on social networks and can be sued by co-workers, competitors, customers, and any individual that views a social media post as defamatory, proprietary, harassing, or libelous. All policies that regulate off-duty conduct apply to social media activity.

Prohibited Activities

The following activities are illustrative of acts that are grounds for disciplinary action:

1. Accessing, transmitting, downloading, printing, or storing information with sexually explicit, pornographic, or obscene content.
2. Downloading or transmitting fraudulent, threatening, intimidating, inflammatory, defamatory, harassing, discriminatory, or otherwise unlawful messages or images.
3. Using the District's electronic communications system in any manner that violates the District's discrimination or harassment policies or commitment to equal employment opportunity.
4. Using the District's electronic communications system for a purpose that is found to constitute, in the District's sole and absolute discretion, a commercial use that is not for the direct benefit of the District.
5. Using the District's electronic communications system in a manner that violates the trademark, copyright, or license rights of any other person, entity, or organization.
6. Blogging, spamming, or streaming on District computers.
7. Transmitting, displaying, storing, or inviting receipt of messages or information which involves election campaigning, requests for charitable or political contributions, advocating one's personal religious beliefs, or any other activity which would constitute solicitation in the workplace.
8. Initiating or sustaining chain letters.
9. Direct and indirect use of the internet and District electronic equipment participation in any gambling or wagering activities of any kind.
10. Publishing links from the District's web page, or posting the District logo, on any employee's personal website or web page without prior written consent.
11. Installing personal software applications, including programs and screensavers, to any District computer without the prior authorization of District management.
12. Copying, transmitting, storing, displaying, or inviting receipt of messages or information that contains confidential, proprietary, or sensitive information pertaining to the District including, but not limited to, engineering, security & safety, human resources, or legal issues.
13. Reading, recording, copying, or listening to messages or information delivered to another employee's e-mail or voicemail without authorization.
14. Sending messages with content that conflicts with any District policies, rules, or other applicable laws.
15. Any use that would be offensive to a reasonable person.

Access Control and Inspection

The District reserves the sole discretion to allow, refuse, or limit by physical and non-physical means, the ability to connect any devices to a District network or infrastructure. The District can and may establish audit trails of use without notice. Such trails will be used to track the attachment of an external device to a PC, and the resulting reports used for investigation of possible breaches or misuse. Access and/or connection to District networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done to identify accounts/computers/mobile devices that may have been compromised by external parties. In all cases, data protection remains the District's highest priority. The District reserves the right, through policy enforcement and any other means necessary, to limit the ability to transfer data to and from specific resources on the District network.

Security

The District will manage security, network, application, and data access centrally using suitable technology. Any attempt to contravene or bypass said security will be deemed an intrusion attempt and access will be terminated. All devices and software for network and data access shall use secure data management. This includes the secure physical control of devices containing District data. In the event of a lost or stolen device, the device will be remotely wiped of all data and locked to prevent access. The District may also remove data no longer deemed appropriate at its sole discretion.

Passwords and other confidential data, as determined by the IT Department, are not to be stored unencrypted on mobile devices. All devices must be protected by a password, and all data stored on the device must be encrypted. Anti-virus software on any additional machines, such as a home PC, which access District data, must be up to date and is the sole responsibility of the user. All connections to the District network through an unmanaged network (i.e. the Internet) will be inspected by the District. Devices representing any threat to the District network or data will not be allowed to connect. Laptops, PCs, or iPad's may only access the District network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection.

Hardware/Software

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed and approved at the sole discretion of the District. Non-approved use of mobile devices to backup, store, and otherwise access any District-related data is prohibited. Modifications of any kind to District-owned and installed hardware or software or installation of mobile applications, without the express approval of the District, are prohibited. This includes, but is not limited to, any reconfiguration of the mobile device. The District will support approved hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software.