



WEED RECREATION & PARKS DISTRICT

161 E. Lincoln Ave

Weed, Ca. 96094

Phone: 530-938-4685

E-mail: weedrec161e.lincolnave@outlook.com Web: www.weedrec.org

POLICY TITLE: Information Technology Acceptable Use

POLICY NUMBER: 2412

POLICY ADOPTION DATE: 9/17/26

POLICY REVISION DATE(S):

2412: Purpose: To provide guidance and direction to our employees about what is acceptable and unacceptable use of business resources. Malicious actors take advantage of situations where acceptable use standards are not clearly defined. This policy defines the rules, responsibilities, prohibited actions, and potential consequences associated with the use and/or misuse of Weed Recreation and Park District's (WRPD) resources. Employees are prohibited from using WRPD's IT resources and supporting peripherals to conduct any malicious acts like mail bombing, flooding and deliberate attempts to overload a system, for example.

As one of WRPD's ambassadors, it is important that your online activities are respectful, responsible and reflect positively on the District. It is prohibited to use either company resources or personal devices to send offensive or explicit text messages or access offensive or explicit websites.

2412.1 IT Device Security: Access to WRPD's IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions of our business's IT systems. Employees must not do the actions below:

- a) Allow anyone else to use their user ID/token and password on any company IT system;
- b) Leave their user accounts logged in while unattended and unlocked;
- c) Use someone else's user ID and password to access WRPD's IT systems;
- d) Leave their password unprotected (e.g. writing it down and leaving it under the laptop);
- e) Perform any unauthorized changes to IT systems or information such as installing peer-to-peer file sharing software, downloading software and games from the Internet, using unauthorized cloud-based file sharing tools, turning off anti-virus software;
- f) Attempt to access data that they are not authorized to use or access;
- g) Exceed the limits of their authorization or specific business need to access systems or data;



WEED RECREATION & PARKS DISTRICT

161 E. Lincoln Ave

Weed, Ca. 96094

Phone: 530-938-4685

E-mail: weedrec161e.lincolnave@outlook.com Web: wwwweedrec.org

- h) Connect any non-company authorized device to the company network or IT systems;
- i) Store company data on any non-authorized business equipment;
- j) Comply with other IT policies.
- k) Give or transfer business data or software to any person or organization outside of the company without leadership approval.

2412.3 Privacy and Data Protections: WRPD obtains and uses sensitive data to conduct our business operations. It is imperative that our employees recognize what data is sensitive, how that data needs to be protected and how it can be used appropriately. It is important that all employees comply with the following:

- a) Do not collect or retain Personally Identifiable Information (PII) any longer than required for business purposes. Our IT team can assist in providing information on data retention schedules;
- b) If you erroneously receive Special Handling or Sensitive PII, report this as a potential confidential information (CI) incident. Do not destroy or remove the data unless instructed by the incident response team. If you erroneously receive other types of PII or confidential information (CI), immediately return or destroy the information;
- c) Safeguard PII and confidential information during transmission and storage by using approved encryption methods such as password-protecting files;
- d) Use only company-issued or approved equipment (including portable media) when storing PII and confidential information;
- e) Confidential information and PII should not be transmitted to/from your personal non-corporate email accounts;
- f) Appropriate measures should be taken at all times to secure working papers or other hard copy files containing confidential information or PII to include customer credit card numbers;
- g) Do not disclose confidential information or PII without appropriate authorization to do so;
- h) Use only company-approved Internet-based services to store Confidential Information or PII or to transfer such information to other;
- i) Hard copy records should be maintained in locked file cabinets, and should be returned to locked file cabinets when not being actively used even if they will be checked out again within a short time;
- j) Ensure measures are taken to secure records overnight;
- k) When emailing, printing or faxing, validate distribution list and/or destination details before sending;
- l) Do not share confidential information or PII over the phone, be careful when answer questions from unknown sources over the phone;



WEED RECREATION & PARKS DISTRICT

161 E. Lincoln Ave

Weed, Ca. 96094

Phone: 530-938-4685

E-mail: weedrec161e.lincolnave@outlook.com Web: wwwweedrec.org

- m) Always confirm you are printing to the correct printer;
- n) Retrieve printing documents immediately from the output tray when using public printers.

2412.4 Use of Wi-Fi: This element of our Acceptable Use Policy covers employee use of Wi-Fi outside of WRPD's Wi-Fi network. Employees shall not use public Wi-Fi using company resources. Access to corporate networks while offsite shall use our virtual private network (VPN) service.

- a) Employees are prohibited from using networks other than the Company's network or service for corporate activities;
- b) Users must use the anti-virus software installed on the device and keep it up to date at all times;
- c) Use of the wireless network is subject to the same guidelines as the company IT governance and security policies.

2412.5 Use of Company IT Resources: This element of our Acceptable Use Policy covers employee use of WRPD's IT resources. Employees may use our corporate resources and Internet access for limited personal use. In no case should this personal use interfere with the completion of job duties and assignments. Employees may use WRPD's resources during break times and lunch periods. See our social media policy about policies concerning posting information about yourself or company activities on social media.

Follow our policy on backing up data to our corporate file management system.

2412.6 Logins and Password: This element of our Acceptable Use Policy covers using passwords to protect company IT resources.

- a) Login password must be a minimum of 8 characters and use upper and lower case letters with numerical digits and special characters;
- b) Employees agree not to write down or share passwords or PINs with others;
- c) Employees agree to comply with password change requirements;
- d) Employees agree not to access the company's IT resources after they have left the company or been terminated. Our IT staff will lock out the employee's account.



WEED RECREATION & PARKS DISTRICT

161 E. Lincoln Ave

Weed, Ca. 96094

Phone: 530-938-4685

E-mail: weedrec161e.lincolnave@outlook.com Web: wwwweedrec.org

2412.7 Personal & Physical Security: This element of our Acceptable Use Policy covers how employee personal security is protected and how physical measures are in place to protect the company's physical assets. Employees shall:

- a) Secure your laptop with a cable lock and do not share the cable lock's combination with others;
- b) Whenever a staff member loses a device, he/she must notify our leadership team immediately to prevent any future loss of data;
- c) When travelling, secure your device in the vehicle's trunk and do not leave it in the trunk overnight;
- d) Always wear your badge or uniform that indicates to our customers you are an employee of WRPD. Do not allow un-badged persons to "tailgate" into secure areas and escort visitors in the workplace at all times;
- e) Do not deface or remove any posted signs, equipment or procedures used to alert and/or inform staff on how to respond to emergencies;
- f) Staff may not introduce weapons of any type and may not use equipment to perform violent acts or issue threats against others in the workplace at any time;
- g) Obtain management approval before using any sort of audio or video equipment to record and/or publish the activities of staff in the workplace;
- h) Staff may only use equipment or supplies for personal use on a limited basis, and usage must not interfere with the completion of required organizational activities;
- i) Staff may not share any physical building access keys, codes or badges to grant unauthorized access to workplace areas;
- j) Before staff complete the off-boarding process, they must return all building access keys and/or badges to the facility security manager.

2412.8 Telework

This element of our Acceptable Use Policy covers how employees can telework and continue to protect company data and systems. All employees must have an approved telework agreement prior to commencing telework.

- a) Make sure your system is using a modern operating system;
- b) Optimize the use of non-privileged accounts to conduct business activities across all devices and limit the use of administrator accounts for software updates;
- c) Install a security suite with anti-virus, anti-phishing, safe browsing, firewall and host-based intrusion prevention/detection capabilities on the device you will be using if it is not a company resource;
- d) Implement the WPA2 protocol on your Wi-Fi network and connect a separate Wi-Fi router to the router received from the service provider to create a separate wireless



WEED RECREATION & PARKS DISTRICT

161 E. Lincoln Ave

Weed, Ca. 96094

Phone: 530-938-4685

E-mail: weedrec161e.lincolnav@outlook.com Web: www.weedrec.org

- network for guests; or optimize the use of a virtual private network (VPN) across all devices as much as possible to connect to the organization's internal network;
- e) Enable the use of Transport Level Security v1.2 to encrypt all Web traffic as much as possible;
 - f) Do not share passwords with others and make sure to configure strong passwords across computing and network devices;
 - g) Only run programs or open email attachments from known and trusted sources, and enable visibility into all filename extensions to help identify potentially malicious files;
 - h) Regularly apply the latest patches to your devices' operating systems and applications;
 - i) Turn off the Wi-Fi adapter on your device when the devices is not in use;
 - j) Disable Java, JavaScript, and ActiveX controls in your Web browser, if possible;
 - k) If possible, disable the use of HTML in email programs by displaying emails as plain text instead;
 - l) Use WRPD's data backup method to regularly backup critical data;
 - m) Maintain a lockbox or locked file cabinet to secure any files containing sensitive information.

2412.9 Bring Your Own Device (BYOD): Employees must follow the requirements below:

- a) It is prohibited to use mobile devices to send offensive or explicit text messages or access offensive or explicit websites;
- b) Your mobile device(s) must be registered and authenticated before you connect to WRPD's network. This allows network administrators to detect unauthorized devices on the network;
- c) You are required to encrypt sensitive data stored on your personal devices with strong encryption. Full device encryption is best, but if that isn't feasible, all sensitive data should be stored in encrypted folders on the device;
- d) Do not install unauthorized applications and regularly backup any corporate data stored on your mobile device;
- e) Upon your departure, you agree to having your personal mobile device wiped clean and factory settings restored on the device you used while at work.

2412.10 Applicability: This policy applies to both temporary and permanent employees and contractors of WRPD.