WEST VALLEY WATER DISTRICT
855 W. Base Line Road, Rialto, CA 92376
PH: (909) 875-1804 FAX: (909) 875-1849

POLICY REVIEW AND OVERSIGHT COMMITTEE MEETING AGENDA

TUESDAY, MAY 23, 2023 - 6:00 PM

NOTICE IS HEREBY GIVEN that West Valley Water District has called a meeting of the Policy Review and Oversight Committee to meet in the Administrative Conference Room, 855 W. Base Line Road, Rialto, CA 92376.

BOARD OF DIRECTORS

President Gregory Young, Chair
Director Kelvin Moore

Members of the public may attend the meeting in person at 855 W. Base Line Road, Rialto, CA 92376, or you may join the meeting using Zoom by clicking this link: https://us02web.zoom.us/j/8402937790. Public comment may be submitted via Zoom, by telephone by calling the following number and access code: Dial: (888) 475-4499, Access Code: 840-293-7790, or via email to administration@wvwd.org.

If you require additional assistance, please contact administration@wvwd.org.

I. CALL TO ORDER

II. PUBLIC PARTICIPATION

The public may address the Board on matters within its jurisdiction. Speakers are requested to keep their comments to no more than three (3) minutes. However, the Board of Directors is prohibited by State Law to take action on items not included on the printed agenda.

III. DISCUSSION ITEMS

1. Updates to the Policy Review and Oversight Committee

2. Information Technology Policies.

IV. ADJOURN

DECLARATION OF POSTING:

I declare under penalty of perjury, that I am employed by the West Valley Water District and posted the foregoing Policy Review and Oversight Committee Agenda at the District Offices on May 18, 2023.

Elvia Dominguez

Elvia Dominguez, Board Secretary

BOARD OF DIRECTORS
POLICY REVIEW AND OVERSIGHT COMMITTEE
STAFF REPORT

DATE: May 23, 2023
TO: Policy Review and Oversight Committee
FROM: Van Jew, Acting General Manager
SUBJECT: INFORMATION TECHNOLOGY POLICIES

BACKGROUND:

West Valley Water District, ("District"), does not have a single, comprehensive Information Technology, ("IT"), policy. Instead, several other policies contain sections that address various IT related issues. Section 2300 of the Personnel Policies and Procedures, (attached as Exhibit A), and Sections 6 and 7 of the Telecommuting Policy, (attached as Exhibit B), primarily address the appropriate use of IT assets. Section H.3. of the Purchase Card Policies and Procedures, (attached as Exhibit C), addresses the purchase of IT assets.

DISCUSSION:

The three policies above were Board approved on 07/01/21, 12/01/22, and 09/03/20 respectively. Staff are reviewing the sections as indicated and will make recommendations for updates as needed. However, staff also proposes that a more comprehensive Information Technology Policy would be appropriate for the District. Therefore, a draft will be prepared and presented to the Safety and Technology Committee.

FISCAL IMPACT:

No fiscal impact.

STAFF RECOMMENDATION:

This agenda item is for information only, no action is required.

Respectfully Submitted,

Van Jew

Van Jew, Acting General Manager

VJ:js

ATTACHMENT(S):

1. Exhibit A - Personnel Policies and Procedures Section 2300
2. Exhibit B - Telecommuting Policy Sections 6 and 7
3. Exhibit C - Purchase Card Policies and Procedures Section H3

EXHIBIT A

Personnel Policies and Procedures
20220701

Section 2300

SECTION 2300
USE OF DISTRICT VEHICLES, EQUIPMENT, AND TOOLS

District equipment and resources may only be used to conduct District business, except for incidental personal use that is consistent with this Policy. As a result, District equipment and resources are non-public forums, and employees shall have no expectation of privacy as to the use or content of such equipment and resources.

All District employees are required to adhere to this Policy.

2301 DISTRICT EQUIPMENT OR RESOURCES

District equipment or resources is any District-owned or supplied item or resource, including, but not limited to: intellectual property (e.g., photographs, plans, drawings, formulas, customer lists, designs, formulas), vehicles, telephones, cell phones, pagers, tools, machines, supplies, copy machines, facsimile machines, desks, office equipment, computers (including hardware and software), file cabinets, lockers, Wi-Fi, internet, intranet, District network, data systems, routers, voice mail, servers, and email or voice mail communications stored in or transmitted through District electronic resources or equipment.

2302 NO EXPECTATION OF PRIVACY

The District periodically and without prior notice, monitors, reviews, accesses, or retrieves data from its equipment or resources, including electronic communications and content contained in or transmitted through District networks or electronic resources.

District employees must provide the agency with the employee's username or password for any District-issued equipment or resource.

The existence of passwords or delete functions does not restrict the District's access. As a result, District employees have no expectation of privacy in their use of any District equipment or resources.

2303 APPROPRIATE USE ONLY – NO MISUSE

Employees may only use District equipment or resources in compliance with District policies. Except as authorized by this Policy, employees are expected to avoid any use or communication which is unrelated to District business, destructive, wasteful, or illegal.

The District has discretion to restrict or rescind employee access to District equipment or resources. The following are examples of misuse of District equipment or resources:

a) Any use that violates applicable law and/or District policies, rules or procedures.

b) Exposing others to material, which is offensive, harassing, obscene or in poor taste. This includes information which could create an intimidating, offensive or hostile work environment.

c) Any use that may create or further a hostile attitude or give offense on the basis of race, color, religion, sex, gender, gender expression, gender identity, national origin, ancestry, citizenship, age, marital status, physical or mental disability, medical condition, genetic information, sexual orientation, veteran status or any other basis protected by law.

d) Communication and/or disclosure of confidential or proprietary District information to unauthorized individuals within or outside of the District.

e) Unauthorized attempts to access or use District data or break into any District or non-District system.

f) Theft or unauthorized transmission or copying of paper or electronic files or data.

g) Initiating or sustaining chain/spam letters, e-mail or other unauthorized mass communication.

h) Misrepresentation of one's identity for improper or illegal purposes.

i) Personal commercial or business activities (e.g. "for sale" notices, personal ads, etc.).

j) Transmitting/accessing obscene material and/or pornography.

k) E-Commerce.

l) Online gambling.

m) Installing or downloading unauthorized software or equipment.

n) Violating terms of software licensing agreements.

o) Using District equipment or resources to access and/or use dating web resources, personal social media, or games of any type.

p) Any unauthorized access to District equipment or resources, including: using keys or key cards; using or disclosing the username or password of another person or employee to gain access to his or her email or other electronic resources; or making District equipment or resources available to others who would otherwise have no authorized access.

q) Using District equipment or resources to speak on the District's behalf without authorization.

r) Interfering with any District security measures.

Additional Security Measures

Employees are responsible for the following:

a) Maintaining the security of District equipment and resources under their control. This includes, but is not limited to, locking District vehicles, securing District PC's, PDA's, smart phones, laptops, and workstations with a password, keeping all passwords secure, logging off when a device is unattended, and not providing access to District information systems either deliberately or through failure to secure system access.

b) Promptly reporting any security breaches or theft of District equipment or resources to their supervisor.

2304 DISTRICT EMAIL ADDRESSES

The District's email system is an official communication tool for District business.

The District establishes and assigns official email addresses to each employee as the District deems necessary. Employees must send all District communications that are sent via email to and from his or her official District email address.

Employees are prohibited from using their private email address (such as Gmail, yahoo, MSN/Hotmail, etc.) when communicating District business via email.

Should an email related to District business be sent to an employee's personal email account, the email should be immediately forwarded to the employee's District email account and responded to accordingly.

1) Incidental Personal Use

Employees may use District telephones, cell phones, internet access, and e-mail for incidental personal communications provided that the use:

a) Is kept to a minimum and limited to break times or non-working hours;

b) Does not interfere or conflict with District operations or the work performance of any District employees;

c) Allows the employee to more efficiently perform District work;

d) Is not abusive, illegal, inappropriate, or prohibited by this Policy (for example, no social media use, no electronic dating, no gaming); and

e) Clearly indicates it is for personal use and does not indicate or imply City sponsorship or endorsement.

2305 USE OF DISTRICT VEHICLES

Due to the need for designated District personnel to respond to emergencies as soon as possible and be available to the public on a 24-hour basis, the General Manager, Assistant General Manager, Director of Governmental & Legislative Affairs, Director of Operations, Director of Engineering, field supervisors, shift operator, and on-call employees shall be assigned a District vehicle to be used for commuting from home to work and from work to home.

The use of a District vehicle for this purpose is a benefit to the District, not the employee; however, per IRS regulations the use of the vehicle for commuting must be calculated as a taxable benefit.

Use of District vehicles for personal use is generally prohibited. However, the District recognizes that the District Vehicle may be used by the standby personnel on occasion for personal errands within the response time area.

Failure to comply shall subject the employee to disciplinary action and/or termination.

2306 PERSONAL USE OF EQUIPMENT AND TOOLS

District-owned equipment and tools shall not be used for personal use.

2307 CELL PHONE USE WHILE DRIVING

In the interest of the safety of our employees and other drivers, the District employees are prohibited from using cell phones, including text messaging, while driving or operating District vehicles or equipment and while driving or operating personal vehicles or equipment while on District business and/or District time.

If your job requires that you keep your District issued cell phone turned on while you are driving and you receive a call, you must use a hands-free device or safely pull off the road to take and engage in the call, and before you conduct District business through the call. Under no circumstances should employees place phone calls or text message while driving or operating equipment or a motor vehicle while on District business and/or District time.

Personal Cell Phone Use

Field personnel will use the District two-way radios to conduct daily business. In emergency situations, cell phones may be utilized for communication purposes.

2308 ELECTRONIC TRACKING TECHNOLOGY

Employees of the District may, in the course of employment, be required to drive and/or ride in a District-owned or leased vehicle equipped with Electronic Tracking Technology.

Electronic Tracking Technology means a technological method or system used to observe, monitor, or collect information, including telematics, Global Positioning System (GPS), wireless technology, or location-based technologies.

Electronic Tracking Technology may include event data recorders (EDR), sensing and diagnostic modules (SDM), or other systems that are used for the purpose of identifying, diagnosing, or monitoring functions related to the potential need to repair, service, or perform maintenance on the District vehicle and/or to capture safety systems-related data for retrieval after a collision or similar incident has occurred.

Electronic Tracking Technology is intended to allow the District to monitor location, elevation, and velocity of its vehicles; and to ensure the vehicles are used in an appropriate and business-related manner.

Electronic Tracking Technology use for public safety greatly enhances job performance, personnel safety, situational awareness, and may provide assistance in time critical scenarios.

Electronic Tracking Technology in District-vehicles may also be used to for other business-related purposes, including, but not limited to, measuring productivity, locating stolen vehicles, providing aid to vehicles that break down, increasing employee safety, managing agency resources effectively, or ensuring that employees are following their routes or assignments.

The District may use Electronic Tracking Technology at the agency's sole discretion. Not all District vehicles are required to have Electronic Tracking Technology.

Utilized for Disciplinary Investigations

The District may utilize Electronic Technology to initiate a disciplinary investigation or discipline of its employees pertaining to the misuse or abuse of their vehicles, inappropriate use of time, speeding or other misconduct. Thus, the documents provided by the Electronic Tracking Technology, if any, could be part of a personnel file and subject to protections afforded the same.

The California Public Records Act may require that the District disclose specified public records. In response to requests for such disclosure, it may be necessary to

examine Electronic Tracking Technology records to determine whether they are public records that are subject to disclosure.

Additionally, the agency may be required to produce information obtained from Electronic Tracking Technology pursuant to a court order, subpoena, or statute.

Employees are prohibited from altering or attempting to alter or disable electronic Tracking Technology in the District's vehicles.

EXHIBIT B

Telecommuting Policy 20221201

Sections 6 & 7

5. All periods of an employee's unavailability must be approved in advance by the supervisor and in accordance with District policy.

6. Employees must promptly notify their supervisor when unable to perform work assignments because of equipment failure or other unforeseen circumstances.

7. Employees shall continue to abide by District policies, practices, procedures and applicable Terms and Conditions of Employment for requests of sick, vacation and other leaves of absences. If an employee becomes ill while Telecommuting, they shall notify their supervisor immediately and record on their timesheet any hours not worked due to incapacitation.

8. Employees must be accessible via telephone, email, and/or network access to their supervisor and other District employees while Telecommuting, as if working at the Central Workplace. Employees shall check their District-related business phone messages and emails on a consistent basis, as if working at the Central Workplace.

9. Employees shall work on a full-time basis, according to their assigned Work Schedule. Employees are required to maintain an accurate record of all hours worked at their Alternative Work Location. Upon the request of their supervisor, an employee should be able to provide a detailed accounting of all hours worked.

D. Employee Wages and Benefits

The duties, obligations, responsibilities, and conditions of a District employee are not changed by Telecommuting. Employee's wages, retirement, benefits, and insurance coverage remain unchanged.

The Telecommuting employee remains obligated to comply with all District rules, policies, practices, and instructions. Violations may result in preclusion from Telecommuting and/or disciplinary action, up to and including termination of employment.

Workers' Compensation benefits will apply only to injuries arising out of and in the course of employment as defined by Workers' Compensation law. The District shall not be responsible for injuries or property damage unrelated to such work activities, including injuries to third persons when said injuries occur at the Alternative Worksite. The District will not be liable for any injuries sustained by visitors or other third-persons at an employee's Alternative Worksite.

6. EQUIPMENT:

A. Electronic equipment needed for employees to perform their work at the Alternative Worksite will be supplied by the District to the extent resources are available and based on operational need. The supervisor, Department Head, and IT Staff will discuss the equipment needed and will have sole discretion in decisions regarding equipment. Equipment supplied by the District is to be used for business purposes only and in accordance with District policies, practices, procedures and applicable Terms and Conditions of Employment.

B. The employee is responsible for ensuring that equipment is used properly. Employees will report to their supervisor any loss, damage, or unauthorized access to District-owned equipment immediately upon discovery of such loss, damage, or unauthorized access.

C. The District will provide for maintenance and repairs to District equipment and retains ownership of all equipment and/or licenses provided.

D. In the event of delay in repair or replacement of equipment or any other circumstance under which it would be ineffective for the employee to telecommute, the employee will return to the District work place.

E. All District-owned equipment issued to an employee must be immediately returned (1) when requested by the District and in good working order, (2) when the Telecommuting Agreement ends, or (3) upon employment separation. Additional equipment needed by the employee to Telework shall be supplied by the employee and at the employee's expense.

F. Should it be required, employees may receive approval to use personal phones, computers, or other equipment for Telecommuting at the discretion of the District. Equipment supplied by the employee, if deemed appropriate by the District, will be maintained by the employee. The District accepts no responsibility for damage or repairs to employee-owned equipment and reserves the right to make determinations as to appropriate equipment, subject to change at any time. Personal equipment used for District work purposes, may be subject to applicable state and federal law.

G. The employee must complete the Authorization to Use District Property at an Alternative Worksite (Appendix B) and thereby agree to take appropriate action to protect the items from damage or theft.

H. The District will provide employees with appropriate office supplies (pens, paper, etc.) as deemed necessary. Employees may obtain the needed supplies when at the District worksite or facility.

I. The District will not be responsible for costs associated with the setup of the employee's home office or Alternative Worksite, such as remodeling, furniture or lighting, nor for repairs or modifications to the home office space. Normal household expenses associated with the Alternative Worksite, such as internet services and utilities (heat, electricity, etc.) are the sole responsibility of the employee and shall be non-reimbursable.

J. Employee's Alternative Worksite must have internet and cell service with sufficient speed/capacity to conduct work via computer and phone.

K. Employees should seek advice from a tax advisor if they have questions concerning the tax implications of Telecommuting. The District is not responsible for substantiating any employee's claim of tax deductions for operation of a Telecommuting office used to perform District work.

7. SECURITY:

A. Consistent with the District's expectations of information security for employees working at a District worksite or facility, Telecommuting employees must ensure the protection of proprietary District and customer information accessible from their Alternative Worksite.

B. Employees shall exercise the same precautions to safeguard electronic and paper information, protect confidentiality, and adhere to the District's records retention policy,

especially as it pertains to the California Public Records Act. Employees must safeguard all sensitive and confidential information (both on paper and in electronic form) relating to District work they access from their Alternative Worksite or transport from the Central Workplace to their Alternative Worksite. Employees must also take reasonable precautions to prevent third parties from accessing or handling sensitive and confidential District information the employee accesses from their Alternative Worksite or transport from the Central Workplace to their Alternative Worksite through the use of locked file cabinets and desks, regular password maintenance, and any other measures appropriate for the job and the environment.

C. Employees shall ensure that all official District documents are retained and maintained according to District policy and procedure in the same manner as if working at the Central Workplace.

D. Employees must return all records, documents, and correspondence to the District upon request from the District.

E. Employees may receive a virtual private network ("VPN") account, as approved by the District. Employees shall take reasonable precautions to ensure their devices (e.g., computers, laptops, tablets, smart phones, etc.) are secure before connecting remotely to the District's network and shall close or secure all connections to District desktop or system resources (e.g., remote desktop, VPN connections, etc.) when not conducting work for the District.

EXHIBIT C

Purchase Card Policies and Procedures 20200903

Section H.3.

ADMINISTRATIVE PROCEDURES

West Valley Water District

APPROVAL DATE	FINANCE POLICIES	POLICY NO.
APPROVED BY: Board of Directors	POLICY TITLE **PURCHASE CARD POLICIES & PROCEDURES**	EFFECTIVE DATE

G. Documentation, Reconciliation and Payment Policy

Any time a purchase is made with the purchase card, whether done over the counter, by telephone or via the internet, a receipt or other similar document shall be retained by the Department as proof of purchase and to provide back-up documentation, if required, for the reconciliation of the purchase. The receipt or other similar document can be used to verify the purchases shown on the cardholder's monthly statement. The receipt should be kept for a period of two years. If for any reason the cardholder does not have documentation of the transaction to provide with the statement, the cardholder should attach an explanation that includes a description of the item, merchant name, and reason for the lack of other supporting documentation, so that supervisors can make informed decisions as to their approvals of purchase card transactions.

H. Card Restrictions

The following list sets forth prohibited purchases with the purchase cards

1. Cash advances through bank tellers or automated teller machines.

2. Purchase of items stocked in the District Warehouse, (i.e., items kept in central stores or items for which the District has a centralized contract such as coffee supplies, paper, and postage), unless required in emergencies.

3. Microcomputer software and hardware (unless approved in writing by the Director of General Services).

4. Personal items even if the employee reimburses the District.