WESA

AGENDA

THE WATER EMPLOYEE SERVICES AUTHORITY ("WESA")
BOARD OF DIRECTORS
REGULAR MEETING
August 26, 2021
4:00 PM

CALL TO ORDER AND ROLL CALL– Edmondson, Burke, Morris, Ryan, Williams

PLEDGE OF ALLEGIANCE AND INVOCATION

ADD-ON ITEMS

APPROVAL OF AGENDA

PUBLIC COMMENT

Any person may address the Board at this time upon any subject not identified on this Agenda, but within the jurisdiction of Water Employee Services Authority; however, any matter that requires action will be referred to staff for a report and action at a subsequent Board meeting. As to matters on the Agenda, an opportunity will be given to address the Board when the matter is considered.

In the interest of public health and safety this meeting will be held as a hybrid (in-person and virtually). To request the opportunity to make a public comment at the meeting, go to https://www.evmwd.com/wesa-publiccomment to complete a Public Comment Request Form prior to the start of the meeting. Please note, individuals have a limit of three (3) minutes to make comments and will have the opportunity when called upon by the presiding officer.

I. CONSENT CALENDAR

Consent Calendar items are expected to be routine and non-controversial, to be acted upon by the Board at one time without discussion. If any Board member, staff member, or interested person requests that an item be removed from the Calendar, it shall be removed so that it may be acted upon separately.

A. Approval of:
   1. Minutes of the Regular Board Meeting of August 12, 2021
   2. Payment Ratification
   3. Extension of Existing Agreement between the Water Employee Services Authority and the Water Employee Services Authority Management Team Association for the Term of One Year
   4. Amendment to Administrative Code Section 1450 - Information Technology Acceptable Use Policy

II. REPORTS

Reports are placed on the Agenda to provide information to the Board and the public. There is no action called for in these items. The Board may engage in discussion on any report upon which specific subject matter is identified, but may not take any action other than to place the matter on a subsequent Agenda.

A. General Manager's Report
B. Legal Counsel's Report

III. DIRECTOR'S COMMENTS AND REQUESTS

Directors' Comments concern Water Employee Services Authority business which may be of interest to the Board. They are placed on the Agenda to enable individual Board members to convey information to the Board and the public. There is no discussion or action required, other than to place the matter on a subsequent Agenda.

IV. INFORMATION ITEMS

A. Reimbursement Disclosure Report of Staff Reimbursements for January - June 2021

V. ADJOURNMENT

Pursuant to the Governor's Executive Orders N-25-20 and N-29-20, and in the interest of public health and safety, this meeting will be conducted as a hybrid (in-person and virtually.) Participants who would like to join this meeting remotely can do so in one of the following ways:

For Online Participation:
Go to: www.zoom.us
Select Join a Meeting
Enter Meeting ID: 837 1375 7929
Meeting Password: 92530

For Call-in Only:
Call: (720) 707-2699
Enter Meeting ID: 837 1375 7929
Meeting Password: 92530

MINUTES OF REGULAR MEETING
WATER EMPLOYEE SERVICES AUTHORITY ("WESA")
BOARD OF DIRECTORS
THURSDAY, AUGUST 12, 2021
4:00 P.M.

The Regular Meeting of the Board of Directors of Water Employee Services Authority was held as a hybrid meeting (teleconference, through a call-in number clearly noted on the meeting Agenda, and in-person) posted in accordance with the Brown Act.

Directors Present
Phil Williams, President
Darcy M. Burke, Vice President
Harvey R. Ryan
Andy Morris
Chance Edmondson

Staff Present
Greg Thomas, General Manager
Michael Maurer, General Counsel
Robert Hartwig, Treasurer
Ganesh Krishnamurthy, Assistant General Manager – Eng. and Operations
Terese Quintanar, District Secretary
Christy Gonzalez, Executive Assistant/Deputy Board Secretary
Susie Evans, Sr. Executive Assistant
Christina Ramirez, Executive Assistant
Skyler Munson, Executive Assistant
Margie Armstrong, Director of Strategic Programs
Tim Collie, Water Operations Manager
Jason Dafforn, Director of Engineering and Water Resources
Greg Morrison, Government Relations Officer
Jennifer Dancho, Director of Human Resources and Safety
Matthew Bates, Engineering Manager
Christina Henry, Community Relations Manager
Parag Kalaria, Water Resources Manager
Darryn Flexman, Interim Director of Information Technology
Wendy Martinez, Records Coordinator
David Smith, Maintenance Manager
Daryl Connor, Lead Facilities Maintenance
Jessie Arellano, Wastewater Operations Manager

Others Present
Public

Approval of: #1.

CALL TO ORDER

The meeting was called to order by President Williams at 6:26 p.m.

APPROVAL OF AGENDA

A motion was made by Director Morris, seconded by Vice President Burke, and carried to approve the Agenda as presented.

PUBLIC COMMENT

The meeting was opened to public comment and there were none.

ITEM I. CONSENT CALENDAR

A. Approval of:
   1. Minutes of the Regular Board Meeting of July 22, 2021
   2. Payment Ratification Report

A motion was made by Director Morris, seconded by Vice President Burke, and carried with Director Edmondson abstaining to:

1. Approve the Consent Calendar as presented.

ITEM II. REPORTS

A. General Manager's Report

Mr. Thomas had nothing to report.

B. Legal Counsel's Report

Mr. Maurer had nothing to report.

ITEM III. DIRECTOR'S COMMENTS AND REQUESTS

There were none.

ITEM IV. CLOSED SESSION

The Board adjourned to Closed Session at 6:29 p.m. to discuss:

A. CONFERENCE WITH LABOR NEGOTIATOR; Agency designated representative: Greg Thomas, Employee Organization: Water Employee Services Authority Management Team Association

The Board reconvened to open session at 6:50 p.m. with nothing to report.

Approval of: #1.

ITEM V. ADJOURNMENT

There being no further business, the meeting was adjourned 6:50 p.m.

Phil Williams, President of the
Board of Directors of the
Water Employee Services Authority

ATTEST:

Terese Quintanar, Board Secretary
to the Board of Directors of the
Water Employee Services Authority

Approval of: #1.

WESA

Print Date: 08/17/2021

Payment Ratification Report

Cash Disbursements for 07/30/2021 through 08/12/2021

Check or Reference #	Payment Date	Paid to Vendor	Payment Description	Pmt Type	Payment Amount
ACH					
2294	08/05/2021	CIGNA HEALTH AND LIFE INS.	MEDICAL COVERAGE - AUGUST 2021	ACH	79,906.54
2295	08/05/2021	COMPLETE GYM SOLUTIONS LLC	EQUIPMENT RENTAL - AUGUST 2021	ACH	1,201.69
2296	08/05/2021	EMPLOYMENT SCREENING SERVICES	EMPLOYMENT SCREENING SERVICES	ACH	170.00
2297	08/05/2021	MELENDEZ, MARIA	CAL PERS LOAN REIMBURSEMENT	ACH	112.22
2298	08/05/2021	US BANK	P CARD PURCHASES – JULY 2021 TRANSACTIONS	ACH	18,258.98
2313	08/12/2021	EMPLOYEE ASSOCIATION	EMPLOYEE ASSOCIATION DUES	ACH	1,760.00
2314	08/12/2021	ISOLVED BENEFIT SERVICES	EE FSA MEDICAL	ACH	3,484.75
2315	08/12/2021	MANAGEMENT TEAM ASSOCIATION	MANAGEMENT TEAM ASSOCIATION DUES	ACH	270.00
CHECKS					
138160	08/05/2021	ACWA JOINT POWERS INS AUTH	HEALTH/VISION COVERAGE - SEPTEMBER 2021	CHECK	183,628.80
138161	08/05/2021	CAREERS IN GOVERNMENT INC	ANNUAL MEMBERSHIP - 08/2021-08/2022	CHECK	1,500.00
138162	08/05/2021	ELSINORE VALLEY MWD	HR RENT – JULY 2021	CHECK	532.00
138163	08/05/2021	HUNTER, LENAI	CERTIFICATION REIMBURSEMENT	CHECK	125.00
138164	08/05/2021	LINCOLN NATL LIFE INS COMP	LIFE/AD&D/LTD INSURANCE - AUGUST 2021	CHECK	10,393.56
138165	08/05/2021	PETTY CASH	REPLENISHMENT OF PETTY CASH - MAY-JULY 2021	CHECK	435.31
138166	08/05/2021	VANTAGEPOINT TRANSFER AGENTS	RHS CONTRIBUTION - EA PPE 07/23/2021	CHECK	2,446.48
138167	08/05/2021	VANTAGEPOINT TRANSFER AGENTS	RHS CONTRIBUTION - MTA PPE 07/23/2021	CHECK	2,017.02
138226	08/12/2021	AFLAC INSURANCE GROUP	AFLAC PRETAX GROUP INSURANCE	CHECK	203.57
138227	08/12/2021	AFLAC	AFLAC PRETAX GROUP INSURANCE	CHECK	856.42
138228	08/12/2021	EMPLOYMENT DEVELOPMENT DEPT	CONFIDENTIAL GARNISHMENT	CHECK	75.00
138229	08/12/2021	GARCIA, ROSALINA	CONFIDENTIAL GARNISHMENT	CHECK	1,147.02
138230	08/12/2021	INDUSTRIAL SAFETY PROFESSIONALS, INC	QUANTITATIVE RESPIRATORY FIT TESTING	CHECK	715.00
138231	08/12/2021	LEGALSHIELD	PRE PAID LEGAL SERVICE	CHECK	26.68
138232	08/12/2021	LINCOLN FINANCIAL GROUP	457 CONTRIBUTION	CHECK	625.00
138233	08/12/2021	LINCOLN NATL LIFE INS COMP	VOLUNTARY LIFE INSURANCE	CHECK	1,379.82
138234	08/12/2021	MARTINEZ, SERGIO	REFUND VOL DEDUCTION	CHECK	4.68
138235	08/12/2021	NATIONWIDE	457 CONTRIBUTION	CHECK	2,816.46
138236	08/12/2021	STATE DISBURSEMENT UNIT	CONFIDENTIAL GARNISHMENT	CHECK	197.53
138237	08/12/2021	STATE DISBURSEMENT UNIT	CONFIDENTIAL GARNISHMENT	CHECK	222.00
138238	08/12/2021	STATE DISBURSEMENT UNIT	CONFIDENTIAL GARNISHMENT	CHECK	222.11
138239	08/12/2021	STATE DISBURSEMENT UNIT	CONFIDENTIAL GARNISHMENT	CHECK	111.69
138240	08/12/2021	STATE DISBURSEMENT UNIT	CONFIDENTIAL GARNISHMENT	CHECK	110.76

WESA

Print Date: 08/17/2021

Payment Ratification Report

Cash Disbursements for 07/30/2021 through 08/12/2021

Check or Reference #	Payment Date	Paid to Vendor	Payment Description	Pmt Type	Payment Amount
138241	08/12/2021	STUART, CHATO	CERTIFICATION REIMBURSEMENT	CHECK	180.00
138242	08/12/2021	TX CHILD SUPPORT SDU	CONFIDENTIAL GARNISHMENT	CHECK	287.54
138243	08/12/2021	VANTAGEPOINT TRANSFER AGENTS	RHS CONTRIBUTION - EA PPE 08/06/2021	CHECK	2,446.48
138244	08/12/2021	VANTAGEPOINT TRANSFER AGENTS	RHS CONTRIBUTION - MTA PPE 08/06/2021	CHECK	2,017.02
WIRE TRANSFERS					
0168406432	08/11/2021	CALIF STATE TAXES	PAYROLL TAXES - PAY PERIOD 2021-08-06	WIRE	23,793.70
01684064322	08/11/2021	CALIF SDI TAXES	PAYROLL TAXES - PAY PERIOD 2021-08-06	WIRE	6,743.69
03109	07/30/2021	FICA WITHHELD	PAYROLL TAXES - PERIOD 2021-07-29 FINAL CHECK	WIRE	44.30
031092	07/30/2021	CALIF STATE TAXES	PAYROLL TAXES - PERIOD 2021-07-29 FINAL CHECK	WIRE	18.81
031093	07/30/2021	CALIF SDI TAXES	PAYROLL TAXES - PERIOD 2021-07-29 FINAL CHECK	WIRE	18.33
03582	08/11/2021	FEDERAL TAX PAYMENTS	PAYROLL TAXES - PAY PERIOD 2021-08-06	WIRE	58,496.80
035822	08/11/2021	FICA WITHHELD	PAYROLL TAXES - PAY PERIOD 2021-08-06	WIRE	17,507.00
10016491942	08/11/2021	CalPERS Survivor - Employee	PERS CONTRIBUTIONS - PAY PERIOD 2021-08-06	WIRE	148.80
100164919422	08/11/2021	CalPERS RETIREMENT CONTRIBUTIONS	PERS CONTRIBUTIONS - PAY PERIOD 2021-08-06	WIRE	115,428.41
10016514673	08/11/2021	CALPERS 457 CONTRIBUTIONS	PERS 457 CONTRIBUTIONS - PAY PERIOD 2021-08-06	WIRE	22,254.45
1576545696	08/05/2021	CALIF STATE TAXES	PAYROLL TAXES - PAY PERIOD 2021-08-05 FINAL CHECK	WIRE	1,842.81
15765456962	08/05/2021	CALIF SDI TAXES	PAYROLL TAXES - PAY PERIOD 2021-08-05 FINAL CHECK	WIRE	223.26
53256	08/05/2021	FEDERAL TAX PAYMENTS	PAYROLL TAXES - PAY PERIOD 2021-08-05 FINAL CHECK	WIRE	4,902.96
532562	08/05/2021	FICA WITHHELD	PAYROLL TAXES - PAY PERIOD 2021-08-05 FINAL CHECK	WIRE	539.54
VIRTUAL PAYMENT PROGRAM					
136	08/12/2021	BOOT BARN INC.	BOOT PURCHASE	VIRTUAL	404.19
137	08/12/2021	TOTAL CARE FAMILY MED CTR LE	PRE-EMPLOYMENT & EMPLOYEE TESTING	VIRTUAL	1,089.00

Reviewed By: _____

Date: 8/17/2021

Approval of: #2.

DATE: August 26, 2021

TO: Board of Directors

FROM: General Manager

SUBJECT: EXTENSION OF EXISTING AGREEMENT BETWEEN THE WATER EMPLOYEE SERVICES AUTHORITY AND THE WATER EMPLOYEE SERVICES AUTHORITY MANAGEMENT TEAM ASSOCIATION FOR THE TERM OF ONE YEAR

BACKGROUND

Due to current economic and environmental conditions, staff has met with the Board Representatives of the Water Employee Services Authority (WESA) Management Team Association (MTA) and both parties have agreed to and recommend an extension of the current Memorandum of Understanding (MOU) in place between WESA and the WESA MTA for the term of one year.

RECOMMENDATION

The General Manager and staff recommend that the Board of Directors:

Approve Side Letter of Agreement No. 2 Between the Water Employee Services Authority and the Water Employee Services Authority Management Team Association, amending Article V, Section 51, of the MOU, effective January 1, 2018, to December 31, 2021, that one additional year be added to extend the existing agreement between WESA and the WESA MTA by one year, with the new ending date of December 31, 2022. The MOU shall remain in full force and effect during the remainder of its term.

ENVIRONMENTAL WORK STATUS

Not applicable.

FISCAL IMPACT

None - within budget

Originated by: J. Dancho – Human Resources
Reviewed by: Terese Quintanar – Administration

Attachments:
Side Letter of Agreemnt No. 2

SIDE LETTER OF AGREEMENT NO. 2 BETWEEN WATER EMPLOYEE SERVICES AUTHORITY AND THE WATER EMPLOYEE SERVICES AUTHORITY MANAGEMENT TEAM ASSOCIATION

This side letter is to the referenced Memorandum of Understanding (MOU), effective January 1, 2018, to December 31, 2021, and amends Article V, Section 51 as follows:

Section 51. Term, Termination and Renewal
That one additional year will be added to extend the existing term of agreement with the new ending date of December 31, 2022.

This side letter agreement is being executed as an integral part of the MOU between the Water Employee Services Authority and the Water Employee Services Authority Management Team Association, effective January 1, 2018, to December 31, 2021. Except as herein modified, the aforesaid MOU shall remain in full force and effect during the remainder of its term.

William Graham President, WESA MTA	Phil Williams President, WESA Board of Directors
Date	Date

Approval of: #3.

DATE: August 26, 2021

TO: Board of Directors

FROM: General Manager

SUBJECT: AUTHORIZE AMENDMENT TO ADMINISTRATIVE CODE SECTION 1450 – INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

BACKGROUND

Section 1450 of the Administrative Code outlines the WESA's computer and network use policy and rules. Being prudent, staff reviewed the policy for relevancy and found that the policy and technology references had become outdated due to ever-changing technological advances and references to once-popular devices that are no longer being used.

Staff updated the policy to allow for more useful and efficient reference and simplified and clarified the language. The proposed amendments to Section 1450 condense the length of the policy (21 pages now are 7 pages) without compromising clarity. It communicates the District's policies regarding the use of Information Technology-related resources, including but not limited to email, the internet, desk and laptop computers and other network resources.

Proposed amendments have been reviewed by Legal Counsel at Best Best and Krieger, LLP and the Director of Human Resources, and the draft policy was found to be in compliance with employment laws.

The proposed amendments were discussed at the Finance and Administration Committee meeting of July 20, 2021, and the Committee and staff recommend approval of the updated policy, and authorization to amend the Administrative Code as appropriate. Staff intends to also recommend the amendments to the EVMWD Board of Directors, for consistency and modernization of EVMWD's Network Policy/Information Technology Acceptable Use Policy.

RECOMMENDATION

The General Manager and staff recommend that the Board of Directors:

1. Authorize Amendment to Section 1450 of the Administrative Code

Approval of: #4.

ENVIRONMENTAL WORK STATUS

Not applicable.

FISCAL IMPACT

Not applicable.

Originated by: Darryn Flexman – - Information Technology
Reviewed by: Terese Quintanar - Administration

Attachments:

Redline draft of Section 1450 of the Administrative Code
Section 1450 -Revised

Approval of: #4.

SECTION 1450. INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY~~NETWORK USE POLICY~~

§ 1451. Purpose.

This policy is designed to establish acceptable and appropriate use of computer equipment, information systems, databases, communications, networks, and other information technology resources at WESA.

~~**Purpose.** To provide guidelines pertaining to employee behavior, access and usage of WESA's network and computer equipment. The procedures and principles represented in this policy apply to all WESA employees, elected officials, volunteers and other affiliates who use WESA provided computer network equipment. The policy also applines to connecting to the District's internal network or related technology resources via any means involving mobile devices that are categorized as Personal Digital Assistants (PDAs). This policy applies to, but is not limited to, all devices that fit the following device classifications:~~

~~Handhelds running the PalmOS, Microsoft Windows CE, PocketPC or Windows Mobile, Symbian, or Mobile Linux operating systems.~~

~~Mobile devices that are standalone (i.e. connectible using wired sync cables and/or cradles.)~~

~~Devices that have integrated wireless capability. This capability may include, but is not limited to, Wi-Fi, Bluetooth, and IR.~~

~~Smartphones that include PDA functionality.~~

~~Any related components of the District's technology infrastructure used to provide connectivity to the above.~~

~~Any third-party hardware, software, processes, or services used to provide connectivity to the above.~~

~~The policy applies to any PDA hardware and related software that could be used to access the District's resources, even if said equipment is not corporately sanctioned, owned, or supplied.~~

§ 1452. Applicability.

This policy applies to all employees (full or part time), elected officials, temporary staff, volunteers, or any other person who utilizes WESA information technology resources, including but not limited to computer hardware, computer networks, software applications, SaaS (Software as a Service), and mobile devices.

~~**§ 1452. Directories.**~~

~~A. Private Directories. All employees are setup with a private directory that can also be accessed by the systems administrator.~~

~~B. Public Directories. All employees are setup with a public directory that can be accessed by any other person assigned to your workgroup. There are also places on the public directory g:\ where WESA staff can store and retrieve files.~~

~~C. Other Directories. Employees should not attempt to gain access to a file or directory that does not pertain to their specific job function. Casual browsing of the network is not permitted.~~

§ 1453. Internet Usage.

A. Use of the Internet by employees of WESA is permitted and encouraged where such use supports the goals and objectives of WESA. However, access to the Internet is a privilege and all employees must adhere to the policies concerning Computer, Email, and Internet usage. Violation of these policies may result in disciplinary and/or legal action, up to and including termination of employment. Employees may also be held personally liable for damages caused by any violations of this policy.

B. Computer, Email, and Internet usage

1. WESA employees are expected to use the Internet responsibly and productively.

2. Incidental and occasional personal use of the Internet is permitted, as long as it does not interfere with the employee's duties. However, such use shall be treated the same as official use, and thus, the user shall have no expectation of privacy when using WESA systems for personal use. As such, personal use is subject to the

Approval of: #4.

same access and review rights as any other use of these systems.

3. All Internet data that is composed, transmitted and/or received by WESA's computer systems is considered to belong to WESA and is recognized as part of its official data. It is therefore subject to disclosure under the California Public Records Act. WESA reserves the right to access the contents of any messages sent or received using WESA equipment or facilities, with or without notice to users. All communications, including email, text and images, can be disclosed to law enforcement or other third parties, without prior consent of the sender or the receiver.
4. The equipment, services and technology used to access the Internet are the property of WESA and WESA reserves the right to monitor Internet traffic and monitor and access data that is composed, sent, or received through its online connections.
5. Emails sent via WESA's email system must not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.
6. All sites and downloads may be monitored and/or blocked by WESA if they are deemed to be harmful and/or not productive to business needs.
7. The installation of software not authorized by the IT department is strictly prohibited.

C. Unacceptable use of the Internet or Email by employees includes, but is not limited to:

1. Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via WESA's email system.
2. Using computers to perpetrate any form of fraud, and/or software, film, or music piracy.
3. Sending communications of confidential WESA information to unauthorized individuals within or outside of WESA.

Approval of: #4.

4. Downloading, copying, or pirating software and electronic files that are copyrighted or without authorization.

5. Conducting a personal/commercial business using WESA resources.

6. Opening an email attachment that you are not expecting to receive. The most destructive viruses to date are email viruses hidden as an attachment.

7. Sending copies of documents in violation of copyright laws.

8. Introducing malicious software onto WESA's network and/or jeopardizing the security of the organization's electronic communications systems.

9. Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.

10. Intentional misrepresentation of one's identity for improper or illegal acts.

11. Revealing your password or access information to WESA equipment or resources to anyone other than Information Technology Department staff.

§ 1453. Introduction.

Computer information systems and networks are an integral part of business at WESA. WESA has made a substantial investment in human and financial resources to create these systems. This policy and its directives have been established in order to:

(1) Protect this investment.
(2) Safeguard the information contained within these systems.
(3) Reduce business and legal risk.
(4) Protect the good name of WESA.

A. Authority. The Information Technology department administers this policy. This policy is currently effective for all WESA employees and computer systems.

B. Contents. The topics covered in this document include:
(1)Statement of responsibilities

Approval of: #4.

~~(2)The Internet~~
~~(3) E-mail~~
~~(4) Computer viruses~~
~~(5) Access codes and passwords~~
~~(6) Computer use~~
~~(7) Brown Act Compliance~~
~~(8) Copyrights and license agreements~~

~~C. Continuance. This policy is a living document and may be modified at any time as the Director of Information Technology or Human Resources, or the Information Systems Group, and approved by the Board of Directors.~~

§ 1454. Access Codes and Passwords.

The confidentiality and integrity of data stored on WESA computer systems must be protected by access controls including but not limited to Multi-Factor Authentication, to ensure that only authorized users have access. This access shall be restricted to only those capabilities that are appropriate to each user's job duties.

A. User Responsibilities. Each User:

1. Shall be responsible for all computer transactions made with their User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they have become known to others. Passwords should not be recorded where they may be easily obtained.
3. Should log out when leaving a workstation for an extended period.
4. Shall not allow any unauthorized person access WESA email, data or resources while accessing WESA resources from a remote location such as home or a hotel. Unauthorized access is a breach of this policy and disciplinary actions will be taken.
5. Shall immediately notify Information Technology staff of any unauthorized use of user's account, and/or any breach, or attempted breach, of security known to user.

~~**§ 1454. Statement of Responsibilities.**~~

~~A. Manager Responsibilities. Managers and supervisors in each department must:~~

(1) Ensure that all appropriate personnel have read, signed, and comply with this policy.
(2) Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

§ 1455. The Internet.

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. To govern employee behavior pertaining to access and usage of publicly accessible computer networks such as the Internet, the procedures and principles presented herein apply to all WESA employees, elected officials, volunteers and other affiliates who use WESA-provided publicly accessible computer networks such as the Internet, regardless of the employee's location when accessing the network.

A. Policy. WESA's policy is to provide computer and communications equipment to those who need it to perform established job responsibilities. If the network user account being used is one provided by WESA, official business is to be conducted via that access. Use of the Internet for personal gain or any other purpose, which is illegal, or against WESA policy or contrary to WESA's best interest is prohibited.

Authorized employees who do access a WESA-provided account on a publicly accessible computer network such as the Internet from a location other than a WESA facility must have their supervisor's written permission to do so. A copy of this written permission must be on file with Human Resources.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive and to protect WESA's interests, the following guidelines have been established for using the Internet.

B. Internet Access is a Privilege.Employees understand that the use of any WESA-provided publicly accessible computer network such as the Internet is a privilege. Unauthorized use of the Internet will result in the loss of access for the user and,

depending on the seriousness of the infraction, may result in disciplinary action up to and including termination.

C. Acceptable Use. Employees using the Internet are representing WESA. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

(1) Using Web browsers to obtain business information from commercial Web sites.
(2) Accessing databases for information as needed.

D. Personal Use. Incidental and occasional personal use of the Internet as covered by this policy may be permitted at the discretion of the division manager and/or department director. However, such use shall be treated the same as official use, and thus, the employee shall have no expectation of privacy when using WESA systems for personal use. As such, personal use is subject to the same access and review rights as any other use of these systems.

E. Unacceptable Use. Employees must not use the Internet for purposes that are illegal, unethical, harmful to WESA, or nonproductive. Examples of unacceptable use are:

(1) Conducting a personal business using WESA resources.
(2) Transmitting any content that is offensive, pornographic, harassing, or fraudulent.
(3) Playing games or gambling is not permissible anytime whether over the Internet or on a stand-alone computer.
(4) Downloading or receiving media files such as MP3s, movies, illegal software. File sharing programs are not permitted on WESA network.
(5) Downloading, receiving via e-mail or brought into WESA via removable media, any type of screen saver, desktop themes, animated characters, etc. Some of the screen savers and desktop themes are not free, and if not purchased by WESA, violates the software copyright law. Also, some of these programs can conflict with other programs existing on the computer.

F. Copyrights. Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements

~~may result in disciplinary action by WESA and/or legal action by the copyright owner.~~

~~G. Monitoring. Information Technology monitors Internet access. Accessing Internet web sites that are deemed unacceptable under this policy will result in disciplinary action up to and including termination.~~

§ 1455. Computer Use.

It is WESA policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

A. Laptops/Tablets. All technology use rules apply to laptop and tablet users. In addition:

1. Portable computer equipment may be assigned on a temporary or permanent basis to certain staff or WESA officials.
2. Remote access to the WESA Network is available and can be permitted with the permission of the Director of Information Technology. Unless authorized by the General Manager, no user shall use this ability to take the place of their attendance at work. However, remote access can be used in those instances when an individual may be off-site and needs to access WESA's network. All rules listed in this policy apply when accessing the WESA network remotely.
3. VPN (Virtual Private Network) connections shall not be installed on any personal computer or device not authorized by the IT department.
4. Access by outside agencies, temporary personnel, interns, volunteers, probationary users, or consultants is not permitted without specific approval of the Director of Information Technology.
5. Maintenance required on laptops or other electronic equipment is to be completed only by or through the IT Department.

Approval of: #4.

6. Any official or approved user needing technical assistance with District-issued equipment, such as laptops, notebooks, tablets, cell phones, or other technology, must provide the equipment to IT staff, at District Headquarters. Staff will not travel to residences or remote locations to attend to equipment or technical needs.

B. User Responsibilities. The directives below apply to all users:

1. Personal computers or other electronic equipment, including but not limited to portable storage devices, shall not be connected to WESA's network.
2. Users shall not expose hardware to environmental hazards, such as food, smoke, liquids, high or low humidity, and must avoid extreme heat or cold.
3. IT is responsible for all equipment installations, disconnections, modifications, and relocations at WESA headquarters. Users are not to perform these activities without authorization from IT.
4. Users shall not take shared portable equipment such as laptop computers out of WESA buildings without the informed consent of their division manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
5. Users should exercise care to safeguard all electronic equipment assigned to them. Users who neglect this duty may be accountable for any loss or damage that may result.
6. IT is not responsible for any data stored on the local computer. Data stored on the local computer cannot be backed up and is not secure.
7. Users are not allowed to "browse" the network and open/read files that do not relate to their specific duties.
8. Users will either log off or lock their workstations when they will be away from the computer for any length of time.
9. Appropriate use should always be legal, ethical, reflect honesty, reflect community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and an individual's right to privacy and to freedom from intimidation, discrimination, harassment, and unwarranted annoyance.

§ 1456. E-Mail.

E-mail is a method of composing, storing, sending and receiving messages over electronic communications systems. This definition includes e-mail that is delivered to or sent from cellular phones, mobile devices (PDAs) and laptops. E-mail is considered a communication of WESA and will be held to the same standards as formal letters or memorandum. Information Technology has the ability and authority to monitor employee e-mail activity as it applies to the normal course of business when there are reasonable grounds to do so per the request of proper management/supervisory staff. Users should not consider Internet e-mail to be either private or secure and should have no expectation of privacy.

A. Internet E-Mail. Every user has the capability to send/receive e-mail via the Internet.

B. User Responsibilities for E-Mail Records Retention. Each user is responsible for determining if data he or she maintains in Microsoft Outlook is an original record that needs to be stored for retention purposes. Any such record must be saved by the user in an appropriate media format (CD, hard copy file, computer, etc.) that allows for the retrieval, production or reproduction of public records. Computer data shall be stored in the form determined by WESA (Word, etc). These records are to be saved in accordance with WESA's records retention policy. As a general rule, data maintained in Microsoft Outlook is not considered a record that requires retention.

C. Employee Responsibility.

(1) Check incoming e-mail several times per day to ensure a timely response in answering unopened mail messages.
(2) Utilize Microsoft Outlook Out of Office feature whenever possible for planned or unplanned absences.
(3) The e-mail system is not intended to be an archival system. Any e-mail that needs to be saved should be printed and filed accordingly
(4) Clean out Inboxes, Sent Items and Deleted Items folders on a regular basis (weekly).
(5) Be aware that all business performed via the District's e-mail system is subject to disclosure under the Public Records Act. Users are strongly advised to conduct only official business on District E-mail accounts.

D. Unacceptable Use. Opening an e-mail attachment, you are not expecting to receive. The most destructive viruses to date are e-mail viruses hidden as an attachment.

(1) Send or receive any sexually oriented messages or images

(2) Send e-mail containing offensive or harassing statements, including comments based on race, color, gender, age, disability, religion, national origin, physical attributes, sexual preferences or political beliefs.

(3) Take actions that cause interference to the network or to the work of others

(4) Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.

(5) Sending messages in an attempt to "flood" receiver's e-mail box.

(6) Sending copies of documents in violation of copyright laws.

(7) Adding background images to an e-mail.

(8) Sending communications of confidential information to unauthorized individuals within or outside of WESA.

(9) Theft or unauthorized copying of electronic files or data.

(10) Intentional misrepresentation of one's identity for improper or illegal acts.

(11) Revealing your password or access information to equipment or resources to anyone other than Information Technology Department staff.

E. Monitoring. Because all computers, software and telecommunication systems remain the property of WESA and are for official use only, all records, files, transmissions, passwords and other products or contents of these systems are not confidential and may be reviewed at any time by WESA management or its designee(s) without prior notification. Therefore, employees shall have no expectation of privacy in any documents or other materials they write, receive, store or send in the use of these systems.

All messages created, sent, or retrieved over the Internet are the property of WESA and may be regarded as public information. WESA reserves the right to access the contents

of any messages sent over its facilities if WESA believes, in its sole judgment, that it has a business need to do so.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. This means, don't put anything into your e-mail messages that you wouldn't want to see on the front page of a newspaper or be required to explain in a court of law.

§ 1457. Access Codes And Passwords.

The confidentiality and integrity of data stored on WESA computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

A. Employee Responsibilities. Each employee:

(1) Shall be responsible for all computer transactions made with his/her User ID and password.
(2) Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they have become known to others. Passwords should not be recorded where they may be easily obtained.
(3) Should log out when leaving a workstation for an extended period.
(4) Accessing WESA resources from a remote location such as home or a hotel will not let any unauthorized person access WESA e-mail, data or resources. Unauthorized access is a breach of this policy and disciplinary actions will be taken.
(5) Shall immediately notify Information Technology staff of any unauthorized use of user's account, and/or any breach, or attempted breach, of security known to user.

B. Supervisor's Responsibility. Managers and supervisors should promptly notify Information Technology whenever an employee leaves the company so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

C. Human Resources Responsibility. The Human Resources Department will notify Information Technology monthly of

associate transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

§ 1458. Computer Use.

It is WESA policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Laptops/Tablets

All technology use rules apply to laptop and tablet users. In addition:

A. Laptops (or similar equipment) are assigned on a temporary or permanent basis to certain staff.

B. Remote access to the Network is available and can be permitted with the permission of the Director of Information Technology and General Manager. It is the responsibility of the user to provide the necessary hardware for connecting to the network. Unless authorized by the General Manager, no user shall use this ability to take the place of his or her attending work. However, it can be used in those instances when an individual may be off-site and needs to access the network.

C. Access by outside agencies, temporary personnel, interns, volunteers, probationary users, or consultants is not permitted without specific approval of the General Manager.

D. All rules listed in this policy apply when accessing the network remotely.

E. Maintenance required on laptops or other electronic equipment is to be completed only by or through the Information Technology Department, at the headquarters building on Chaney Street.

Any official or approved user needing technical assistance with District-issued equipment, such as laptop, notebook, tablet, cell phone, or other technology, must provide the equipment to the Information Technology staff at the Administrative Headquarters. Staff will not travel to residences or remote locations to attend to equipment or technical needs. Reasonable

~~training related assistance can be provided after an appointment is arranged, to be held at the EVMWD Headquarters building~~

~~Employee Responsibilities~~

~~The directives below apply to all employees:~~

~~(1) Diskettes, Zip disks and CDs should be stored out of sight when not in use. Highly sensitive or confidential data must be locked in a cabinet or desk drawer.~~

~~(2) Diskettes, Zip disks and CDs should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.~~

~~(3) Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). A surge suppressor should protect other computer equipment.~~

~~(4) Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.~~

~~(5) Since Information Technology is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities. This does not apply to temporary moves of portable computers for which an initial connection has been set up by Information Technology.~~

~~(6) Employees shall not take shared portable equipment such as laptop computers out of WESA buildings without the informed consent of their division manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.~~

~~(7) Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.~~

~~(8) All data will be stored on the file server. Each employee will have his or her own private folder to store data on the server. Data will not be stored on the local computer (C: and/or D: and/or E: drives). Information Technology is not responsible for any data stored on the local computer. Data stored on the local computer cannot be backed up and is not secure.~~

~~(9) Modems are not to be installed/used without the knowledge of Information Technology. External modems must be turned off when not in use.~~

(10) Employees are not allowed to "browse" the network and open/read files that do not relate to their specific duties.

(11) Users will either log off or lock their workstations when they will be away from the computer for any length of time. Users can also set their screen saver to use the "password protected option" and set the wait time for no longer than 10 minutes.

(12) Appropriate use should always be legal, ethical, reflect honesty, reflect community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and an individual's right to privacy and to freedom from intimidation, discrimination, harassment, and unwarranted annoyance. Appropriate use of computing and networking resources includes, but it's not limited to, instruction; independent study; authorized research; communications; and other official work of the District.

§ 1459. Compliance with the Ralph M. Brown Act.

As the use of computers and electronic message systems continues to expand, public officials increasingly rely on e-mail as a form of communication. The utilization of these systems provides a convenient and quick method for public officials to communicate with constituents and staff. However, the use of e-mail, as well as other collaborative means of electronic communication, among members of the legislative bodies raises questions regarding compliance with the Ralph M. Brown Act (Gov. Code sec. 54950 et seq.), California's open meeting law. By establishing and following a uniform policy that will apply to Board Members, these officials will be more effective in complying with the Brown Act. In order to protect EVMWD, WESA, and Board Members, the following policy regarding the use of e-mail and other collaborative means of electronic communication shall be followed:

(1) No approved user, Board Member or Committee Member shall e-mail a majority of members of the Board or any Committee about any item that is within the subject matter jurisdiction of that legislative body.

~~(2) E-mail communication among less than a majority of Board Members about any matter that is within the subject matter jurisdiction of that legislative body should not occur and is strongly discouraged.~~

~~(3) No approved user, Board Member or Committee Member shall knowingly participate in any form or collaborative means of electronic communication (i.e., posting to a website, web blog, SharePoint site, etc.) where his or her participation would cause there to be a majority of members of the respective legislative body discussing any item that is within the subject matter jurisdiction of that legislative body. For purposes of this provision "knowingly" means that the person knows or reasonably should know, that his or her participation would result in a majority of a legislative body discussing an item within the subject matter jurisdiction of that legislative body.~~

~~(4) To avoid non-compliance with the Ralph M. Brown Act, Board Members are prohibited from sending, receiving and/or reading electronically produced messages during meetings.~~

~~(5) Cell phones must be turned off while the meeting is in session. If a Board Member is expecting an urgent call, his or her cell phone can remain on and in the possession of the Board Secretary. If such a call is received, the meeting may be adjourned for a short recess at the direction of the Board President.~~

~~(6) Personal communication devices (including PDA's or devices with PDA function ability) must be turned off and put away during meetings.~~

§ 1456. Monitoring Computer, Internet and Email Use.

Because all computers, software and telecommunication systems remain the property of WESA and are for official use only, all records, files, transmissions, passwords and other products or contents of these systems are not confidential and may be reviewed at any time by management or its designee(s), without prior notification. Such monitoring may include conducting reviews of the contents of email messages sent and received, electronic files, websites visited on the Internet, and any other use of WESA's computer and email systems and equipment.

Therefore, users shall have no expectation of privacy or confidentiality in any documents or other materials they write, receive, store or send in the use of these systems.

Approval of: #4.

§ 1457.60 Copyrights aAnd License Agreements.

WESA and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose WESA and the responsible employee(s) to civil and/or criminal penalties.

A. WESA Information Technology is exclusively responsible for installing and supporting all software on WESA computer equipment and electronic devices.

B. Information Technology shall maintain records of software licenses owned by WESA and shall periodically scan WESA computers to verify that only authorized software is installed.

C. User Responsibilities. Users shall not:

1. Install software unless authorized by Information Technology.
   Only software that is licensed to or owned by WESA is to be installed on WESA computers.
2. Copy software unless authorized by Information Technology.
3. Download software unless authorized by Information Technology.

D. Violations. Violations of this policy may result in disciplinary action, up to and including termination.

~~A. Scope. This directive applies to all software that is owned by, or licensed to, WESA, or developed using WESA resources by employees or vendors.~~

~~B. Installation and Support of WESA Software. WESA Information Technology is exclusively responsible for installing and supporting all software on WESA desktop and laptop computers.~~

~~WESA Information Technology relies on installation and support to provide software and hardware in good operating condition to users so that they can best accomplish their tasks.~~

C. Information Technology Responsibilities. Maintain records of software licenses owned by WESA.

(1) Periodically (at least monthly) scan company computers to verify that only authorized software is installed.

D. Employee Responsibilities. Employees shall not:

(1) Bring software from home and use it on their computer.
(2) Install or play games on their computer.
(3) Install software unless authorized by Information Technology. Only software that is licensed to or owned by WESA is to be installed on WESA computers.
(4) Copy software unless authorized by Information Technology.
(5) Download software unless authorized by Information Technology.

Employee shall: Upon termination of employment, the employee must uninstall any Microsoft "Work at Home" (WAH) licenses that may have been purchased by WESA for employees to perform WESA work at home.

E. Violations. Violations may result in disciplinary action in accordance with WESA policy. Failure to observe these guidelines may result in disciplinary action by WESA depending upon the type and severity of the violation, whether it causes any liability or loss to WESA, and/or the presence of any repeated violation(s).

F. Civil Penalties. Violations of copyright law expose WESA and the responsible employee(s) to the following civil penalties:

(1) Liability for damages suffered by the copyright owner
(2) Profits that are attributable to the copying
(3) Fines up to $100,000 for each illegal copy

G. Criminal Penalties. Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b))," expose the company and the employee(s) responsible to the following criminal penalties:
(1) Fines up to $250,000 for each illegal copy
(2) Jail terms of up to five years

Approval of: #4.

§ 1458. Use of Electronic Signatures.

Electronic signatures installed on WESA-issued equipment are to be utilized for WESA business purposes only.

§ 1459. Return of Equipment.

Upon termination of employment with WESA all computer equipment or electronic devices issued shall be returned to Human Resources.

At the end of service as an elected official of WESA, officials shall return all computer equipment or electronic devices issued to them to the Board Secretary.

ATTACHMENT A

Acknowledgment of Computer Usage and Security Policy

By signing below, I acknowledge that I have read and fully understand WESA's Information Technology Acceptable Use Policy.

~~This form is used to acknowledge receipt of, and compliance with, WESA Computer Usage and Security Policy.~~

~~Procedure. Complete the following steps:~~

~~(1) Read the Computer Usage and Security Policy.~~
~~(2) Sign and date in the spaces provided below.~~
~~(3) Return this page to your immediate supervisor, or the Human Resources Department.~~

~~Signature. By signing below, I agree to the following terms:~~

~~(1) I have received and read a copy of the "Network Use Policy" and understand the same;~~
~~(2) I understand and agree that any computers, software, and storage media provided to me by WESA contains proprietary and confidential information about WESA and its customers or its vendors, and that this is, and remains, the property of WESA at all times;~~
~~(3) I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at WESA), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;~~
~~(4) I agree that if I leave WESA for any reason, I shall immediately return to WESA the original and copies of any and all software, computer materials, or computer equipment that I may have received from WESA that is either in my possession or otherwise directly or indirectly under my control.~~

Employee signature: _____

~~Employee name: _____~~

Approval of: #4.

Date: _____ Department: _____

~~§ 1461. WESA Stationery.~~

~~A. Acceptable Uses- Employees~~

- ~~Communications and information exchanges, by authorized personnel as determined by the General Manager, to outside agencies directly relating to WESA Business;~~
- ~~Communications for Board Members relating to official WESA Business, sub or standing committees of the Board of Directors;~~
- ~~Outside of this policy, miscellaneous uses of stationery must receive prior authorization by the General Manager~~

~~B. Noncompliance. Internal discipline, up to and including discharge, may be appropriate in some cases of non-compliance with this policy.~~

~~C. Acceptable Uses- Board of Directors~~

- ~~Communications and information exchanges to outside agencies directly relating to WESA Business, as determined appropriate by the Board President;~~
- ~~Communications with WESA Legal Counsel~~
- ~~Outside of this policy, miscellaneous uses of stationery must receive prior authorization by the Board President~~

~~D. Noncompliance. Board Members shall not use WESA's seal, trademark, stationery or other indicia of WESA's identity, or facsimile thereof, in any solicitation for political contributions contrary to state or federal law. WESA Stationery may not be used for private correspondence. Violations of this Policy will be handled by the full Board of Directors.~~

SECTION 1450. INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

§ 1451. Purpose.

This policy is designed to establish acceptable and appropriate use of computer equipment, information systems, databases, communications, networks, and other information technology resources at WESA.

§ 1452. Applicability.

This policy applies to all employees (full or part time), elected officials, temporary staff, volunteers, or any other person who utilizes WESA information technology resources, including but not limited to computer hardware, computer networks, software applications, SaaS (Software as a Service), and mobile devices.

§ 1453. Internet Usage.

A. Use of the Internet by employees of WESA is permitted and encouraged where such use supports the goals and objectives of WESA. However, access to the Internet is a privilege and all employees must adhere to the policies concerning Computer, Email, and Internet usage. Violation of these policies may result in disciplinary and/or legal action, up to and including termination of employment. Employees may also be held personally liable for damages caused by any violations of this policy.

B. Computer, Email, and Internet usage

1. WESA employees are expected to use the Internet responsibly and productively.

2. Incidental and occasional personal use of the Internet is permitted, as long as it does not interfere with the employee's duties. However, such use shall be treated the same as official use, and thus, the user shall have no expectation of privacy when using WESA systems for personal use. As such, personal use is subject to the

Approval of: #4.

same access and review rights as any other use of these systems.

3. All Internet data that is composed, transmitted and/or received by WESA's computer systems is considered to belong to WESA and is recognized as part of its official data. It is therefore subject to disclosure under the California Public Records Act. WESA reserves the right to access the contents of any messages sent or received using WESA equipment or facilities, with or without notice to users. All communications, including email, text and images, can be disclosed to law enforcement or other third parties, without prior consent of the sender or the receiver.
4. The equipment, services and technology used to access the Internet are the property of WESA and WESA reserves the right to monitor Internet traffic and monitor and access data that is composed, sent, or received through its online connections.
5. Emails sent via WESA's email system must not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images.
6. All sites and downloads may be monitored and/or blocked by WESA if they are deemed to be harmful and/or not productive to business needs.
7. The installation of software not authorized by the Information Technology department is strictly prohibited.

C. <u>Unacceptable use of the Internet or Email by employees includes, but is not limited to:</u>

1. Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via WESA's email system.
2. Using computers to perpetrate any form of fraud, and/or software, film, or music piracy.
3. Sending communications of confidential WESA information to unauthorized individuals within or outside of WESA.

Approval of: #4.

4. Downloading, copying, or pirating software and electronic files that are copyrighted or without authorization.

5. Conducting a personal/commercial business using WESA resources.

6. Opening an email attachment that you are not expecting to receive. The most destructive viruses to date are email viruses hidden as an attachment.

7. Sending copies of documents in violation of copyright laws.

8. Introducing malicious software onto WESA's network and/or jeopardizing the security of the organization's electronic communications systems.

9. Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities.

10. Intentional misrepresentation of one's identity for improper or illegal acts.

11. Revealing your password or access information to WESA equipment or resources to anyone other than Information Technology Department staff.

§ 1454. **Access Codes and Passwords.**

The confidentiality and integrity of data stored on WESA computer systems must be protected by access controls including but not limited to Multi-Factor Authentication, to ensure that only authorized users have access. This access shall be restricted to only those capabilities that are appropriate to each user's job duties.

A. User Responsibilities. Each User:

1. Shall be responsible for all computer transactions made with their User ID and password.

2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they have become known to others. Passwords should not be recorded where they may be easily obtained.

3. Should log out when leaving a workstation for an extended period.

Approval of: #4.

4. Shall not allow any unauthorized person access WESA email, data or resources while accessing WESA resources from a remote location such as home or a hotel. Unauthorized access is a breach of this policy and disciplinary actions will be taken.

5. Shall immediately notify Information Technology staff of any unauthorized use of user's account, and/or any breach, or attempted breach, of security known to user.

§ 1455. Computer Use.

It is WESA policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

A. Laptops/Tablets. All technology use rules apply to laptop and tablet users. In addition:

1. Portable computer equipment may be assigned on a temporary or permanent basis to certain staff or WESA officials.

2. Remote access to the WESA Network is available and can be permitted with the permission of the Director of Information Technology. Unless authorized by the General Manager, no user shall use this ability to take the place of their attendance at work. However, remote access can be used in those instances when an individual may be off-site and needs to access WESA's network. All rules listed in this policy apply when accessing the WESA network remotely.

3. VPN (Virtual Private Network) connections shall not be installed on any personal computer or device not authorized by the IT department.

4. Access by outside agencies, temporary personnel, interns, volunteers, probationary users, or consultants is not permitted without specific approval of the Director of Information Technology.

Approval of: #4.

5. Maintenance required on laptops or other electronic equipment is to be completed only by or through the Information Technology Department.

6. Any official or approved user needing technical assistance with District-issued equipment, such as laptops, notebooks, tablets, cell phones, or other technology, must provide the equipment to Information Technology staff, at District Headquarters. Staff will not travel to residences or remote locations to attend to equipment or technical needs.

B. User Responsibilities. The directives below apply to all users:

1. Personal computers or other electronic equipment, including but not limited to portable storage devices, shall not be connected to WESA's network.

2. Users shall not expose hardware to environmental hazards, such as food, smoke, liquids, high or low humidity, and must avoid extreme heat or cold.

3. The Information Technology department is responsible for all equipment installations, disconnections, modifications, and relocations at WESA headquarters. Users are not to perform these activities without authorization from Information Technology staff.

4. Users shall not take shared portable equipment such as laptop computers out of WESA buildings without the informed consent of their division manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.

5. Users should exercise care to safeguard all electronic equipment assigned to them. Users who neglect this duty may be accountable for any loss or damage that may result.

6. Information Technology is not responsible for any data stored on the local computer. Data stored on the local computer cannot be backed up and is not secure.

7. Users are not allowed to "browse" the network and open/read files that do not relate to their specific duties.

Approval of: #4.

8. Users will either log off or lock their workstations when they will be away from the computer for any length of time.

9. Appropriate use should always be legal, ethical, reflect honesty, reflect community standards, and show restraint in the consumption of shared resources. It should demonstrate respect for intellectual property; ownership of data; system security mechanisms; and an individual's right to privacy and to freedom from intimidation, discrimination, harassment, and unwarranted annoyance.

§ 1456. Monitoring Computer, Internet and Email Use.

Because all computers, software and telecommunication systems remain the property of WESA and are for official use only, all records, files, transmissions, passwords and other products or contents of these systems are not confidential and may be reviewed at any time by management or its designee(s), without prior notification. Such monitoring may include conducting reviews of the contents of email messages sent and received, electronic files, websites visited on the Internet, and any other use of WESA's computer and email systems and equipment.

Therefore, users shall have no expectation of privacy or confidentiality in any documents or other materials they write, receive, store or send in the use of these systems.

§ 1457. Copyrights and License Agreements.

WESA and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose WESA and the responsible employee(s) to civil and/or criminal penalties.

A. WESA Information Technology is exclusively responsible for installing and supporting all software on WESA computer equipment and electronic devices.

Approval of: #4.

B. Information Technology shall maintain records of software licenses owned by WESA and shall periodically scan WESA computers to verify that only authorized software is installed.

C. User Responsibilities. Users shall not:

1. Install software unless authorized by Information Technology.
   Only software that is licensed to or owned by WESA is to be installed on WESA computers.
2. Copy software unless authorized by Information Technology.
3. Download software unless authorized by Information Technology.

D. Violations. Violations of this policy may result in disciplinary action, up to and including termination.

§ 1458. Use of Electronic Signatures.

Electronic signatures installed on WESA-issued equipment are to be utilized for WESA business purposes only.

§ 1459. Return of Equipment.

Upon termination of employment with WESA all computer equipment or electronic devices issued shall be returned to Human Resources.

At the end of service as an elected official of WESA, officials shall return all computer equipment or electronic devices issued to them to the Board Secretary.

Approval of: #4.

ATTACHMENT A

Acknowledgment of Computer Usage and Security Policy

By signing below, I acknowledge that I have read and fully understand WESA's Information Technology Acceptable Use Policy.

Employee signature: _____

Date: _____ Department: _____

Approval of: #4.

DATE: August 26, 2021

TO: Board of Directors

FROM: General Manager

SUBJECT: REIMBURSEMENT DISCLOSURE REPORT OF STAFF REIMBURSEMENTS FOR JANUARY - JUNE 2021

BACKGROUND

In accordance with Government Code Section 53065.5, "each special district, as defined by subdivision (a) of Section 56036, shall at least annually, disclose any reimbursement paid by the district within the immediately preceding fiscal year of at least one hundred dollars ($100) for each individual charge for services or product received. 'Individual charge' includes, but is not limited to, one meal, lodging for one day, transportation or a registration fee paid to any employee or member of the governing body of the district. The disclosure requirement shall be fulfilled by including the reimbursement information in a document published or printed at least annually by a date determined by that district and shall be made available for public inspection."

The total expenses reported on the attached Reimbursement Disclosure Report for January to June 2021 is $5,522.88.

The expense information is being presented in order to comply with State law; no action is recommended.

RECOMMENDATION

The General Manager and staff recommend that the Board of Directors:

1. No action at this time. This is an informational item.

ENVIRONMENTAL WORK STATUS

Not applicable.

FISCAL IMPACT

• Within Budget – Not applicable.

Originated by: Samantha Tran – Finance
Reviewed by: Scott Thompson – Finance

Attachments:

WESA Reimbursement Disclosure Report January to June 2021.

INFORMATION ITEMS #A.

WATER EMPLOYEE SERVICES AUTHORITY
REIMBURSEMENT DISCLOSURE REPORT
JANUARY - JUNE 2021

Name	Check Date	Description	Amount	Total
Allen, P	1/14/2021	Certification Reimbursement	205.00	205.00
Allen, P	2/18/2021	Certification Reimbursement	221.63	221.63
Amezcua	5/20/2021	Boot Purchase Reimbursement	300.00	300.00
Arellano	4/15/2021	Certification Reimbursement	180.00	180.00
Barron	5/13/2021	Boot Purchase Reimbursement	300.00	300.00
Burke	4/29/2021	Boot Purchase Reimbursement	282.76	282.76
Cabrera	4/15/2021	Boot Purchase Reimbursement	300.00	300.00
Dill	3/25/2021	Boot Purchase Reimbursement	140.02	140.02
Dill	4/22/2021	Boot Purchase Reimbursement	159.98	159.98
Garland	6/17/2021	Boot Purchase Reimbursement	256.63	256.63
Garland	6/24/2021	Certification Reimbursement	524.98	524.98
Grieser	6/24/2021	Certification Reimbursement	100.00	100.00
Ibarrola	3/4/2021	Boot Purchase Reimbursement	294.76	294.76
Krishnamurthy	6/28/2021	Certification Reimbursement	180.00	180.00
Lopez	1/7/2021	Boot Purchase Reimbursement	228.38	228.38
Lyon	1/14/2021	Boot Purchase Reimbursement	206.63	206.63
MacGill	5/4/2021	Certification Reimbursement	160.00	160.00

INFORMATION ITEMS #A.

Name	Check Date	Description	Amount	Total
MacGill	6/10/2021	Boot Purchase Reimbursement	200.00	200.00
McCullough	2/4/2021	Boot Purchase Reimbursement	250.11	250.11
Moss	1/28/2021	Membership Reimbursement	192.00	192.00
Moss	2/25/2021	Certification Reimbursement	195.00	195.00
Olivo	5/27/2021	Certification Reimbursement	100.00	100.00
Ruzek	3/11/2021	Boot Purchase Reimbursement	145.00	145.00
Soria	2/28/2021	Boot Purchase Reimbursement	300.00	300.00
Tejeda	5/20/2021	Certification Reimbursement	100.00	100.00
		Total	**5,522.88**	**$ 5,522.88**

INFORMATION ITEMS #A.