MENDOCINO COUNTY EMPLOYEES RETIREMENT ASSOCIATION

PORTABLE ELECTRONIC DEVICE POLICY

I. PURPOSE AND BACKGROUND

This Policy is intended to provide Trustees and staff with guidelines and specific requirements for securely employing portable electronic devices in the conduct of Mendocino County Employees Retirement Association (MCERA) business. The Policy represents trustee and staff recognition of their primary fiduciary obligation to the members and beneficiaries of the plan.

The Policy reinforces the proper use of portable devices, and timely destruction of any confidential information that may be stored on such devices. The Policy assists in identifying and avoiding situations that might compromise the confidentiality of member information entrusted to Trustees and staff for decision making purposes.

This policy is intended to increase awareness and is not intended to cover every possible situation. Common sense should be exercised at all times.

II. POLICY GUIDELINES

A. All Electronic Devices

1. All devices used in the conduct of MCERA business must be equipped with security software to insure that unauthorized individuals will not access potentially sensitive information. This includes enabling any password protection built into the system. Unattended devices must be locked. In addition, users must use all reasonable steps necessary to keep the device safe and secure at all times.

2. Portable electronic devices may remotely access the MCERA network only through remote access systems approved by MCERA.

3. County provided email accounts must be used to conduct MCERA business. Also, confidential email or data files cannot be sent outside the county email system unless the email is adequately encrypted, password protected or otherwise secured.

4. The electronic versions of any confidential information may not be transferred from MCERA approved portable electronic devices to any other electronic devices for any purpose.

5. Trustees and staff agree to delete all confidential information from portable electronic devices as soon as possible once such information is no longer needed for decision making purposes.

6. In order to avoid inadvertent violations of open meeting laws, the Trustees may not use portable electronic devices, whether issued by MCERA or otherwise, to communicate with each other during a meeting of the Board. Further, consistent with law and MCERA's other policies, a majority of the Trustees may not communicate with each other, either at the same time or serially, regarding MCERA matters, outside of noticed Board meetings.

7. Trustees and staff are responsible for the security of the device, all associated equipment and all data. Trustees and staff must immediately report any lost or stolen portable electronic equipment or data to the Executive Director as soon as such loss or theft is discovered. It must also be understood that in the event of loss or theft, the device may be remotely wiped and any personal information stored on the device will be lost. Users are responsible for backing up any personal information; business information should not be backed up.

B. Devices Purchased by MCERA

1. Authorization to periodically use portable electronic devices purchased by MCERA, as well as all associated equipment and software, is limited to and for the purpose of conducting MCERA business. Trustees and staff may make reasonable and limited personal use of MCERA computer resources, systems and equipment. Such personal use is allowed as long as such use does not involve inappropriate uses. Examples of inappropriate use of MCERA computer resources include but are not limited to:

    a. Conducting partisan and/or non-partisan political activity;

    b. Creating and exchanging advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail;

    c. Sending messages or accessing data with content that violates any MCERA policies, rules or other applicable laws;

    d. Sending messages or accessing data that contain inappropriate, defamatory, obscene, harassing, or illegal material;

    e. Sending information that violates or unlawfully infringes on the rights of any other person (including but not limited to copyrights and software licenses);

f. Restricting or inhibiting other authorized users from using the system;

g. Conducting business for personal profit or gain, or other inappropriate conduct as defined in the Mendocino County Internet, E-Mail and Computer Usage Policy;

h. Attempting to hide the identity of the sender or represent the sender as someone else.

2. Trustees and staff have no expectation of privacy with regard to their use of such devices. The devices may be subject to search as permitted or required by law.

3. MCERA portable electronic devices are not solely assigned to individual Trustees and staff but are resources to be used on an as needed basis. MCERA is entitled to and will require such devices to be returned to MCERA for routine maintenance and to ensure that they are being used only in a manner that is consistent with these policies. Board and staff members must return MCERA portable electronic devices to the MCERA Executive Director upon their termination of Trusteeship or MCERA employment.

4. MCERA portable electronic devices are not for the general personal use of the Board member or staff employee or any other person or entity. Trustees and staff will not permit anyone else to use this MCERA property for any purpose. Passwords and/or accounts should not be shared with anyone.

C. Devices Not Purchased by MCERA

Trustees and staff may choose to utilize a portable electronic device not owned by MCERA in the conduct of MCERA business. To the extent applicable, for any period such device is used to conduct MCERA business, said device will be considered a County device, and the user is responsible for compliance with County computer use policies.

1. Trustees and staff will identify to the Executive Director portable electronic devices used for MCERA business.

2. Trustees and staff have no expectation of privacy with regard to their use of portable electronic devices in the course of doing MCERA business. The devices may be subject to search as permitted or required by law.

3. Devices purchased by Trustees and staff will not be subject to maintenance and inspection except as needed to configure the device and to maintain the security and software required for MCERA business.

4. Trustees and staff shall not allow any other person or entity to use the device if the device has confidential information stored on it.

5. Trustees and staff may download other documents, data, and programs without consent of the MCERA Executive Director, as long as these items do not negate any required security measures or interfere with required business software. However, only legally acquired and licensed software may be used to conduct MCERA business.

D. Email Security

"Cyber hygiene" greatly impacts user security. By implementing specific standards that have been widely adopted in the industry, MCERA can ensure the integrity and confidentiality of internet-delivered data, minimize spam, and better protect MCERA membership, staff and trustees.

1. MCERA Trustees are required to use the county issued Outlook, @mendocinocounty.org or .gov, email address when conducting all MCERA business.

2. Email authentication (Two-Factor Authentication, 2FA) must be enabled and used when accessing email the first time from any new device.

3. The use of personal email is not permitted.

III. POLICY REVIEW

This Policy is subject to change in the exercise of the Board's judgment. The Board will review this policy at least every three years to ensure that it remains relevant and appropriate and consistent with state and federal laws and regulations.

IV. POLICY HISTORY

The Board adopted this policy on April 20, 2016
The Board reviewed and amended this policy on October 18, 2017
The Board reviewed and amended this policy on October 21, 2020
The Board reviewed this policy on August 16, 2023