



DRAFT

MPWMD RESOLUTION NO. 2019-17

**ADOPTING THE MONTEREY PENINSULA
WATER MANAGEMENT DISTRICT ELECTRONIC
COMMUNICATIONS POLICY**

WHEREAS, Section 6250 et. seq., of the California Government Code has been interpreted to include in the definition of a public record forms of electronic communications such as email, text messages, voice mail and other electronic writings (electronic communications); and

WHEREAS, the California Supreme Court in the *City of San Jose v. Superior Court* (2017) 2 Cal.4th 608 ruled that electronic writings related to the public's business are public records even where they have been sent, received or stored in a personal account or device; and

WHEREAS, in March 2019, the Monterey Peninsula Water Management District (District) adopted a Records Retention Schedule (RRS) to establish a procedure for the retention and destruction of certain District documents and communications including email, text messages, voice mail and other electronic writings; and

WHEREAS, the District desires to establish an Electronic Communications Management Policy (Policy) to establish procedures for review, retention, and destruction of electronic communications, which will be used in conjunction with the RRS; and

WHEREAS, this action does not constitute a "Project" as that term is defined under the California Environmental Quality Act (CEQA) Guideline Section 15378, as it is an organizational or administrative activity that will not result in direct or indirect physical changes in the environment.

NOW, THEREFORE, THE BOARD OF DIRECTORS OF THE MONTEREY PENINSULA WATER MANAGEMENT DISTRICT DOES RESOLVE AS FOLLOWS:

Section 1. The District Board of Directors hereby approves the MPWMD Electronic Communications Policy **Attachment 1**, attached hereto and incorporated herein by this reference.

Section 2. With the consent of the District Counsel and General Manager, updates are hereby authorized to be made to the Electronic Communications Policy and Email Retention Procedures without further action by the Board of Directors of the Monterey Peninsula Water

Management District. The General Manager shall report to the Board of Directors on any amendments to the Policy approved in the previous year.

Section 3. This resolution shall become effective immediately upon its passage and adoption.

On a motion of Director _____ and second by Director _____ the foregoing resolution is duly adopted this 18th day of November 2019 by the following vote.

AYES: Directors

NOES:

ABSENT:

I David J. Stoldt, Secretary to the Board of Directors of the Monterey Peninsula Water Management District, do hereby certify that the foregoing Resolution No. 2019-17 was duly adopted on the 18th day of November, 2019.

Witness my hand and seal of the Board of Directors this _____ day of _____, 2019.

David J. Stoldt, Secretary to the Board of Directors

MPWMD ELECTRONIC COMMUNICATIONS MANAGEMENT POLICY

November 4, 2019

SCOPE -- This policy applies to all e-mail, text messages, voice mail, instant messaging, and other forms of electronic communications relating to conduct of the public's business that are created, sent, received or stored on personal devices, systems or accounts, or District-owned devices, systems or accounts. This policy is implemented in consideration of the provisions of Government Code §6250 et seq. pertaining to the availability and accessibility of public records.

COMPLIANCE IS MANDATORY -- All District employees, officials and Directors must comply with this policy. The term "employees" includes contract employees/volunteers that work at the District office.

POLICY -- All electronic communications must be analyzed to determine:

- (a) Whether the communication is a record relating to the conduct of the public's business that has administrative, legal, financial or historical value and must be retained for a specific period of time before it is destroyed, or retained permanently, according to the District's Records Retention Schedule; or
- (b) Whether the communication is identified in the District's Records Retention Schedule as a disposable or draft item and no retention is required, as the item is not related to the public's business, is of a transitory or non-substantive nature, or is interagency or intra-agency memoranda not retained in the ordinary course of business.

RETENTION PERIODS -- The District's Records Retention Schedule identifies types of records (record categories) and the minimum length of time a record must be retained before it is moved to permanent storage or destroyed. Electronic communications must be retained according to the Records Retention Schedule.

RETENTION CATEGORIES

- **Permanent:** Records required by law to be retained permanently and records designated by the General Manager as permanent.
- **Perpetual:** Records retained for an indefinite period of time until a trigger event takes place, the record is then stored for a mandated retention period and disposed of according to the Records Retention Schedule. For example, email related to audits, or contracts must be retained until the audit is complete, or the project terminates. Following that triggering event, a mandated retention period begins and the email must be moved onto the District's central electronic file folders u/drive for storage until the retention period ends.
- **Time Specified:** Many record categories on the Records Retention Schedule are associated with a specific retention period, for example 2 years or 5 years. The record may be destroyed when the retention period has expired.
- **No Retention Required:** No administrative, legal, fiscal, or archival requirements for retention. These are transitory messages that convey information of limited importance and can be deleted immediately.

PERSON RESPONSIBLE TO DETERMINE RETENTION AND FILE

- Communication created internally - originator of the communication is responsible to determine retention and file.

- Communication received from an external source - primary recipient is responsible to determine retention and file.
- If it is not clear who the primary recipient is, the persons who received the communication should confer and decide who will retain or destroy the message. The other recipients should not retain the communication.
- Chain email – the entire email chain must be retained; however, duplications within the email chain need not be retained.

DIRECTORS – PROCEDURE FOR RETENTION OF ELECTRONIC COMMUNICATIONS

The District does not issue Directors communication devices nor does it provide systems or accounts for storage of electronic communications. Therefore, Directors must analyze District-related communications sent or received on their personal devices, systems or accounts, and then: (1) transmit those eligible for retention to the Executive Assistant for retention in the District's files; or (2) retain those eligible for retention on the Director's personal device, system or account.

STAFF - PROCEDURE FOR RETENTION OF ELECTRONIC COMMUNICATIONS/ ATTACHMENTS

- Email shall be retained according to the District's Email Retention Procedures
- Email or other electronic communications, including attachments, may be moved to the employee's District electronic file folders and retained for the required retention period
- Email or other electronic communications, including attachments, may also be moved to the District central electronic file folders and retained for the required retention period. Forward to records staff.
- Attachments only may also be forwarded to records staff for retention in the District's central electronic file folders.

DESTRUCTION OF ELECTRONIC COMMUNICATIONS – An electronic communication is considered destroyed as soon as it is moved into the user's deleted items folder or deleted from a user's mailbox or account. A communication considered destroyed is not a recoverable public record.

PRIVACY – Electronic communications sent or received on District-owned devices, systems or accounts are not private. They may be accessed and monitored by others, may be released to the public, and may be subject to discovery proceedings in legal actions. All District-related electronic communications sent or received on a personal device, system or account, or downloaded to a personal device, system or account are subject to review and disclosure.

RECORDS SEARCH ON PERSONAL DEVICES OR ACCOUNTS/DIRECTOR OR EMPLOYEE

If a personal device, system or account must be searched to accommodate a Public Records Act request or legal discovery, the owner or designee shall review the personal device, system or account for responsive records. If no responsive records are found, the owner or designee shall submit a signed affidavit stating that a search was done and no responsive records exist. If responsive records do exist, they shall be submitted to the Executive Assistant, along with a signed affidavit stating that a search was conducted and responsive records are provided. Responsive records should be submitted in the original format, as a PDF, or as printouts with all metadata including distribution information: the names of all recipients, and the dates and times sent or received.

SEPARATION FROM DISTRICT/DIRECTOR OR EMPLOYEE -- Before departing from service or employment with the District, the Director or employee shall search personal electronic devices,

systems and accounts for records eligible for retention. If no responsive records are found, a signed affidavit will be submitted as described under Records Search on Personal Devices or Accounts. If eligible Records are found, they will be submitted to the Executive Assistant along with an affidavit as described under Records Search on Personal Devices or Accounts. The IT Manager will sever the former employee's access to District email.

After an employee separates from the District, messages that have accumulated in the former employee's Mailbox will be retained according to email folder default or tagged retention periods. The manager or supervisor will determine where incoming mail will be routed, and may also grant another staff person access to the Mailbox.

LEGAL HOLDS – When automatic deletion of District email must be temporarily halted to ensure records are available to search in response to a Public Records Act request or legal discovery, the IT Manager will place a hold on Mailboxes of employees that must conduct a search of their files. When the search is complete, if no responsive records are found, the owner or designee will submit a signed affidavit stating that a search was done and no responsive records exist. If responsive records do exist, they will be submitted to the Executive Assistant, along with a signed affidavit stating that a search was conducted and responsive records are provided. The hold will be removed from the affected Mailbox upon receipt of the affidavit.

LEAVE HOLDS – If an employee will be away from the office, and upon request the IT Manager will place a hold on automatic destruction of messages in the employee's Mailbox. The employee must submit to the IT Manager a request form signed by the employee's manager or supervisor that specifies the start and end date of the hold.

POLICY COMPLIANCE – Directors and employees will receive training on the Electronic Communications Management Policy within 30 days of joining the Agency. Management has the right to review electronic communications on District-owned devices to ensure compliance with this policy. If a user does not adhere to the policy, additional training will be provided.

AMENDMENTS TO POLICY – This policy may be amended by approval of the General Manager. Each year at the January meeting of the Board of Directors, the General Manager shall report on any amendments to the policy approved in the previous year.