ADMINISTRATIVE MEMORANDUM
COUNTY OF SAN MATEO

NUMBER: F-2

SUBJECT: Email Policy

RESPONSIBLE DEPARTMENT: Information Services Department (ISD)

APPROVED: _____ **DATE:** June 25, 2019

Michael P. Callagy, County Manager

This memorandum replaces an earlier version of Memorandum F-2, which was last updated on November 7, 2018. In order to ensure countywide compliance and uniformity, all other individual departmental policies regarding the appropriate use of email shall be superseded by this memo.

1. Purpose

This policy outlines the proper use of email resources available to County of San Mateo's Workforce Members (employees, contractors, vendors, interns, extra-help, and any party who provides services or work for the County will be collectively known as "Workforce Members" for the purposes of this document) to ensure that County-provided email services are used in compliance with applicable laws and County policies. Workforce Members who use email services should familiarize themselves with this policy including its explanation of County email privacy and security issues. By complying with this policy, County Workforce Members can ensure that disruptions to the County 's email services are minimal and that the County can continue to manage email in an efficient manner.

2. Scope

This policy applies to all County Workforce Members who accesses or use the County's email system, all equipment that is owned or leased by the County, and to all connections to the County network inclusive of wired, wireless, mobile, and remote connections.

The policy is intended comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as amended and the California Public Records Act.

3. Policy

Email is a means of transmitting written communications electronically. The purpose of email is to communicate between individuals and groups and to promote the effective and efficient use of time and resources to carry out County business. Only County provided email accounts shall be used to conduct County business. As custodians of resources entrusted to them by the public, County Workforce Members should be mindful of how to most appropriately utilize these resources so that other County Workforce Members are not deprived of access to useful resources necessary to perform their duties. Use of third-party email services (such as Gmail or Yahoo mail), including the auto-forwarding of County email to such third-party email services to conduct County business is prohibited.

A. Email Privacy

Email messages sent and received on the County email system are intended for County business use. County Workforce Members shall have no right or expectation of privacy in any email message drafted, sent, or received on the County's email system and the County reserves the right to read, monitor, audit, and delete all such email messages.

Supervisors and managers shall have the right to review any email message drafted, sent, or received on the County email system by any employee supervised by them at any time and for any reason. The request for such review shall be made, in writing, through ISD for administrative access. The Information Services Department (ISD) monitors the use of the County 's email systems and may report to individual departments on usage and suspected misuse of email. For more detailed information on the County's IT Security Policy, refer to the County's Information Technology Security Policy.

B. Email Security

Every County workforce member will be required to use their network password to access their email account and must secure their account with passwords that either meets or exceeds the County 's password requirements. In the event that a workforce member is required to view another's email as part of his or her job duties, that workforce member may be granted permission to access that email via a proxy without violating this policy.

C. Appropriate Email Use

Appropriate use of email includes, but not limited to, the following:

- providing or requesting information regarding County business (e.g. meeting notification, budget issues, etc.);
- transmitting small documents or files (as opposed to printing and mailing the document);
- referencing documents or attachments with the use of a link to the document as it exists on a file sharing platform or within a document management system;

- general announcements within the scope of the sender's job responsibilities (e.g. health and fitness information sent by the Wellness Coordinator); and
- informational announcements from department heads or other designated individuals that need to be communicated to County Workforce Members (e.g. "Spare the Air Day").

D. Inappropriate Email Use

Inappropriate use includes, but not limited to, the transmission of messages containing:

- protected Health Information (PHI) in a manner that is inappropriate and/or violates HIPAA and/or state or county-level regulations protecting PHI, including the transmission of PHI to any party outside the County without the use of encryption levels consistent with HIPAA standards and/or state or County-level regulations;
- information that may be damaging to the County, its Workforce Members, its customers, or clients without a legitimate business need to any party outside of the County;
- any material or comment that is discriminatory, offensive, defamatory or harassing;
- the promotion of or participation in illegal activities;
- copyright infringing material(s);
- items of a political nature or having to do with political activities
- use of County email for the purposes of political action, union elections, personal attacks on other County staff, or any lengthy exchanges unrelated to a legitimate work purpose is prohibited;
- formal or informal corrective action or other personnel actions sent to the subject of the action;
- use of email messages to indicate acceptance to an agreement when signed documents are required (the use of email to distribute documents for signature is acceptable);
- use of a disguised identity when sending email messages.
- Use of, or access to, another person's account without permission.
- unauthorized use of County mailing lists;
- creating or forwarding "chain letters," "pyramid schemes," or monetary recruitments of any type;
- membership or participation in non-work-related mailing lists using County email IDs;
- forwarding of County email to a non-County email account; (should there be a business need to access County email outside of the workplace, email may be accessed through their Office365 account or refer to Administrative Memo B-19, for mobile devices); and
- use of email as a file transfer or sharing mechanism for messages that meet or exceed Message Size Limits that prevents the delivery of other messages and affecting service performance for all Workforce Members (Workforce Members should include a link to the document as an alternative to attaching documents to an email when possible).

E. Email Management

The maintenance of a maximum mailbox size of less than 100GB is the responsibility of the workforce member and includes all folders, subfolders, and containers that reside within the email account including the workforce member's deleted items folder.

F. Mailing Lists

County Email Group Lists
Use of countywide mailing list is restricted to department IT staff and other individuals designated by the department heads. Departments shall establish procedures for the review and approval of all messages transmitted using this list.

Non-County Email Group Lists:
The subscription to any non-County mailing list must be work related. The workforce member must also be aware of how to unsubscribe from the list and is responsible for doing so in the event that his or her current email address changes.

G. Unsolicited Email

As a result of email systems becoming a primary means of distributing computer malware, SPAM, and phishing attempts, the County has taken appropriate actions to filter and to relieve the email system of unsolicited email as well as to restrict incoming email to protect the County's computer systems.

Workforce Members shall treat all unsolicited email with suspicion, particularly email received from the Internet (i.e., non-County email addresses) or those emails requesting the workforce member's log-in information and passwords. Questions regarding the authenticity and integrity of an email it should be referred to department's Information Technology staff or to ISD through ISD Service Desk Ticketing System (ServiceNow) so that it can be reviewed and/or deleted from the workforce member's account.

H. Health Insurance Portability and Accountability Act (HIPAA) Compliance

All departments, or divisions thereof, that are designated as health care components of the County, shall make all received email messages that contain Personally Identifiable Health Information (PHI) a part of the patient's medical record as required, store them in a secure fashion similar to medical record storage, or dispose of them in a manner to protect patient confidentiality. Email messages containing PHI will be treated with the same degree of confidentiality as are other parts of the medical record. Refer to County Administrative Memos B-25, B-26, and B-27 for complete information regarding the County's policies on PHI and HIPAA.

Workforce Members who transmit sensitive information, including PHI, to any authorized recipient outside the County must ensure that the email is encrypted at a level consistent with HIPAA standards. Workforce Members may set the message classification to confidential.

All email containing PHI, Personally Identifiable Information (PII), or other sensitive information must include the following confidentiality statement:

> "This email message, including any attachments, is for the sole use of intended recipient(s) and may contain confidential and protected information. Any unauthorized review; use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message."

I. Signature Block Usage

An email signature block is a block of text that can be automatically, or upon demand, appended to an email message. A common practice is to have one or more lines containing some brief information about the author of the message.

The use of the email signature block shall be limited to sender 's name, title, County of San Mateo, department, address, telephone, County website, and HIPAA confidentiality statement, if required. This information must comply with the County' s Identity and Style Guide

The email signature block should not include personal details, quotations, or graphics that are unrelated to County business.

J. Email Retention

Email messages are temporary communications and the email system (with the exception of archived email subfolders as set forth below) is not intended to be used as a means of records storage. To the extent that email messages which are generated or received through the County' s computer systems constitute business records to be retained pursuant to the County' s (or a department's) records retention policy, such email messages shall be retained as set forth below. Email messages that do not otherwise serve a business purpose (including, but not limited to, draft communications, administrative communications, etc.) shall be routinely discarded. For that reason, each workforce member who uses the County email system has the same responsibility for their email messages as they do for any document they obtain in the course of their official duties and must decide which communications should be retained for business or legal reasons and which should be discarded. If a workforce member has any questions regarding if an email should be retained as a business record, he or she should seek guidance from his/her supervisor and/or department head who may consult with legal counsel as necessary.

Email messages in *all* default folders of a workforce member's mailbox will be

automatically deleted after two (2) years. Automatically deleted emails will be accessible in emergency situations for a period of thirty (30) days after they are deleted from the workforce member's mailbox.

Email messages that constitute records to be retained for business or legal reasons may be saved in excess of two (2) years in any of the following ways: (1) saved in Rich Text Format (RTF) or Portable Document Format (PDF) and then transferred to electronic filing systems or other media for long-term storage in accordance with the department's regular filing and storage procedures; (2) affirmatively "dragged and dropped" or "cut and pasted" into email subfolders created by the workforce member (the workforce member must select the particular retention period that applies to any created subfolders (i.e. one year, two years, ten years, indefinitely, etc.)); or (3) printed in hard copy and filed or stored as appropriate. Any email subfolders created by the workforce member within Microsoft Exchange will, along with the workforce member's inbox including any migrated mail, count toward the user's 100GB mailbox space limitation as outlined in Section E of this policy.

Workforce Members should seek guidance from their department heads to determine the specific time requirements applicable to records and electronic correspondence generated, received and/or maintained by their department in accordance with their department's records retention policy. Workforce Members are strongly encouraged to review the email content of subfolders on a regular basis and to delete any content for which retention is not required.

Regardless of countywide or departmental records retention requirements, email and other electronic correspondence pertaining to a threatened or actual legal action must be retained until the litigation is concluded. It is the responsibility of the department involved, or County Counsel, to notify ISD in writing, of the need for the hold on electronic communications.
The use or creation of local personal archive files (such as Outlook.pst files) is strictly prohibited and may not be configured on County equipment.

K. Deletion of Workforce Member's Account

Following the termination of the workforce member's employment, the email accounts may continue to be accessed by their department directors or appropriate designees in order to continue to conduct County operations.

When a workforce member is no longer working for the County, it is the responsibility of that department to immediately notify ISD. The terminated workforce member's mailbox may remain in the system for as long as thirty (30) calendar days. To maintain a mailbox for longer than thirty (30) calendar days, the workforce member's department head must request an extension in writing with the ISD Service Desk.

L. Back-up of Data

Backup services for the County's email provided by Microsoft provide

Workforce Members with "Deleted Item Recovery" available to restore items that have been deleted from any email folder within thirty (30) days. No other email retrieval options will be available.

4. Consent to Policy

Use of the County's email system constitutes consent to this policy.

5. Other County Policies

The County has other policies that address specific areas of information security including policies on Internet use and portable computing. Departments may have internal email policies relevant to the subject matter associated with the specific work of the department. These policies are cumulative and in the event of conflict, the policies providing the County with the greatest level of security apply. Additionally, County policies concerning employee conduct such as the prohibition of sexual or other harassment apply to use of email.

6. Policy Enforcement

Violations will be investigated, and abuse of this policy may result in disciplinary action up to and including dismissal from County employment. For inappropriate release of PHI, the disciplinary action(s) contained in the County's Protected Health Information Sanction Policy will apply.

7. Revision History

Effective Date	Changes Made
April 16, 1999	Policy established
March 24, 2003	Policy updated
April 28, 2003	Policy updated
March 26, 2007	Policy updated
April 27, 2015	Policy updated
October 3, 2017	Policy updated
November 7, 2018	Policy updated
June 25, 2019	Policy updated