



## ADMINISTRATIVE MEMORANDUM COUNTY OF SAN MATEO

**NUMBER: F-2**

**SUBJECT:** E-Mail Policy

**RESPONSIBLE DEPARTMENT:** Information Services Department (ISD)

**APPROVED:**   
John L. Maltbie, County Manager

**DATE:** April 27, 2015

---

### 1. Policy Purpose

This policy outlines the proper use of E-mail resources available to County of San Mateo Workforce Members in order to assure that County-provided E-mail services are used in compliance with applicable laws and County policies. Users of E-mail services should familiarize themselves with this policy including its explanation of County E-mail privacy and security issues. By complying with this policy, County Workforce Members can ensure that disruptions to the County's E-mail services are minimal and that the County can continue to manage E-mail in an efficient manner.

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

This policy replaces Administrative Memorandum F-2, which was last updated in 2007. In order to ensure countywide compliance and uniformity, all other individual departmental policies regarding appropriate E-mail use, including the countywide Human Resources E-mail policy revised in April 2003, shall be superseded by this memo.

### 2. Policy Scope

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.

This policy applies to all County Workforce Members, 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.

### **3. Policy**

E-mail is a means of transmitting written communications electronically. The purpose of E-mail is to communicate between individuals and groups and to promote the effective and efficient use of time and resources in order to carry out County business. Only County provided E-mail accounts shall be used to conduct County business. Use of third party E-mail services (such as Gmail or Yahoo mail), including the auto-forwarding of County E-mail to such third party E-mail services to conduct County business is prohibited.

#### **A. E-mail Privacy**

E-mail messages sent and received on the County E-mail System are intended for County business. Workforce Members shall have no right or expectation of privacy in any E-mail message drafted, sent, or received on the County E-mail System and the County reserves the right to read, monitor, audit, and delete all such E-mail messages. The County's E-mail Administrators may override Workforce Members' passwords to the County E-mail System without prior notification to the Workforce Member of such action. Similarly, Supervisors and Managers shall have the right to review any E-mail message drafted, sent, or received on a County E-mail System by any employee supervised by them at any time and for any reason. Information Services monitors the use of the County's E-mail systems and may report to individual departments on usage and suspected misuse of E-mail. For more detailed information on the County's IT Security Policy, users may visit: <http://intranet.co.sanmateo.ca.us/blog/it-security-policy/>

#### **B. E-mail Security**

Every user must have a unique E-mail user-ID in order to identify the communications of specific users. Every user must have an E-mail password to secure their account that meets or exceeds the County's password requirements. E-mail passwords are to be kept private and not shared with others including fellow Workforce Members. In the event that a Workforce Member is required to view another's E-mail as part of his or her job duties, that Workforce Member may be granted permission to access that E-mail via a proxy without violating this Policy.

#### **C. Examples of appropriate E-mail Use**

1. Providing or requesting information regarding County business (e.g. meeting notification, budget issues, etc.)
2. Transmitting small documents or files (as opposed to printing and mailing the document)
3. 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.
4. General announcements within the scope of the sender's job responsibilities (e.g. health and fitness information sent by the Wellness Coordinator)



5. 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. Examples of Inappropriate E-mail Use include, but are not limited to, the transmission of messages containing:**

1. 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
2. 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.
3. Any material or comment that is discriminatory, offensive, defamatory or harassing
4. Promotion of or participation in illegal activities
5. Copyright infringing material(s)
6. Items of a political nature or having to do with political activities
7. Use of County E-mail 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.
8. Formal or informal corrective action or other personnel actions sent to the subject of the action
9. Use of E-mail messages to indicate acceptance to an agreement when signed documents are required (the use of E-mail to distribute documents for signature is acceptable)
10. Use of a disguised identity when sending E-mail messages.
11. Use of, or access to, another person’s account without permission.
12. Unauthorized use of County mailing lists
13. Creating or forwarding “chain letters,” “pyramid schemes,” or monetary recruitments of any type
14. Membership or participation in non-work related mailing lists using County E-mail IDs
15. Auto forwarding of County E-mail to a personal E-mail account. Should there be a business need to access County E-mail outside of the workplace, please refer to Administrative Memo B-19, which allows some Workforce Members the ability to receive County E-mail on County-provided or personally owned devices.
16. Use of E-mail as a file transfer or sharing mechanism for messages that meet or exceed Message Size Limits. Message Size Limits are necessary to prevent large messages from blocking delivery of other messages and affecting service performance for all users. Messages that are larger than the system limit cannot be sent or received. Users should include a link to the document as an alternative to attaching documents to an E-mail when possible.

## **E. E-mail Management**

When the County's E-mail system is migrated from the Groupwise System to the Microsoft Exchange E-mail platform, maintenance of a maximum mailbox size of less than 50GB (equivalent to approximately 150,000 average sized text E-mails) is the responsibility of the user. This 50GB limit includes all folders, subfolders, and containers that reside within an E-mail account (mailbox) including a user's trash folder. ISD is unable to unilaterally extend the size of an individual user's mailbox. In the event that a user's e-mail box is at capacity (i.e. 50GB) or is nearing capacity, the user shall notify his or her supervisor in order to resolve the situation without interruption to the user's work.

## **F. Mailing Lists**

### County E-mail Group Lists

The Countywide "All Employees" mailing list is the consolidation of all departmental "All Employees" mailing lists. Use of this mailing list is restricted to department E-mail/LAN (Local Area Network) Administrators and other individuals designated by Department Heads. Departments shall establish procedures for the review and approval of all messages transmitted using this list.

### Non-County E-mail Group Lists:

If a user subscribes to a non-County mailing list, then such E-Mail group list must be work related. The Workforce Member also must be aware of how to unsubscribe from the list and is responsible for doing so in the event that his or her current E-mail address changes.

## **G. Unsolicited E-mail**

The widespread use of E-mail provides an easy way to distribute harmful content. E-mail systems have become a primary means of distributing computer malware, SPAM, and phishing attempts. The County takes appropriate actions to filter and restrict incoming E-mail in order to protect the County's computer systems and to relieve the County's E-mail system of as much unsolicited E-mail as possible.

E-mail users should treat all unsolicited E-mail with suspicion, particularly E-mail received from the Internet (i.e. non-County E-mail addresses) or those E-mails requesting user log-in information and passwords. If the user is unsure of the authenticity and integrity of an E-mail it should be referred to department Information Technology staff through the ISD Help Desk, and, after review by ISD, deleted from the user's account.

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

All departments, or divisions thereof, which are designated as health care components of the County shall make all received E-mail messages which contain Personally Identifiable Health Information (PHI) a part of the patient's medical record as appropriate or store them in a secure fashion similar to medical record storage or dispose of them in a manner to protect patient confidentiality. E-mail messages containing PHI will be treated with the same degree of confidentiality as are other parts of the medical record. For



complete information regarding the County's policies on PHI and HIPAA please see County Administrative Memos B-25, B-26, and B-27.

The transmission of sensitive information, including PHI, to any party outside the County must be encrypted at a level consistent with HIPAA standards, by ensuring that the E-mail is encrypted. Users may set encryption by including "#sec#" in the subject line of the message or by setting the message classification to confidential. By indicating that the E-mail contains secure information with the "#sec#" notation, the user ensures that servers will encrypt the message so that it can be safely delivered to non-County E-mail addresses.

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

"This E-mail 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 E-mail and destroy all copies of the original message."

#### **I. Signature Block Usage**

An E-mail signature block is a block of text that can be automatically, or upon demand, appended to an E-mail 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 E-mail signature block must 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: [http://blogs.co.sanmateo.ca.us/communicationsportal/wp-content/uploads/sites/16/2014/07/140213\\_SMC\\_Style-Guide\\_13.pdf](http://blogs.co.sanmateo.ca.us/communicationsportal/wp-content/uploads/sites/16/2014/07/140213_SMC_Style-Guide_13.pdf)

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

#### **J. E-mail Retention**

E-mail messages are temporary communications and the E-mail system (with the exception of archived E-mail subfolders as set forth below) is not intended to be used as a means of records storage. To the extent that E-mail 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 E-mail messages shall be retained as set forth below. E-mail 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 has the same responsibility for their electronic mailbox 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 whether an E-mail should be retained as a business record, he or she should seek guidance from their supervisor and/or Department Head who may consult with legal counsel as necessary.

Following the County's migration to Microsoft Exchange, E-mail messages in *all* default folders of a user's mailbox will be automatically deleted after ninety (90) days. Automatically deleted E-mails will be accessible in emergency situations for a period of thirty (30) days after they are deleted from the user's mailbox. E-mail messages that constitute records to be retained for business or legal reasons may be saved in excess of ninety (90) days 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 E-mail subfolders created by the user (the user 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 E-mail subfolders created by the user within Microsoft Exchange will, along with the user's inbox including any migrated mail, count toward the user's 50GB mailbox space limitation as outlined in Section E of this policy.

Workforce members should seek guidance from their department heads in order 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 E-mail 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, E-mail 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 User Accounts**

Workforce members should understand that, following a termination of their employment, their E-mail accounts may continue to be accessed by their department directors or appropriate designees in order to continue to conduct County operations after their departure.

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**

Back-up systems are for disaster recovery purposes and are not for departmental records retention. However, the County does access backup media periodically to restore accidentally lost data. Retention is the responsibility of the originator/sender of the message. Back-up media is generally not retained more than three (3) weeks.

Following the County's migration from its current Groupwise E-mail system to Microsoft Exchange, Microsoft will provide backup services for the County's E-mail. As part of those services, mailbox users will have "Deleted Item Recovery" available to them so that they can restore items that have been deleted from any E-mail folder within thirty (30) days. No other E-mail retrieval options will be available.

#### **4. Consent to Policy**

Use of the County E-mail 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 E-mail 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 Workforce Members' use of E-mail.

#### **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 contained in the County's Protected Health Information Sanction Policy will apply.

#### **7. Definitions**

<b>Terms</b>	<b>Definition</b>
County Network	As used here "County network" includes the County's information network backbones, department Local Area Networks (LAN), and all devices that attach, directly or indirectly, to the networks including remote attachments.

Mailbox Size Limits	The GroupWise system's various mailbox size limitations are a function of departmental standards and/or limitations on storage availability. After the County migrates to the Microsoft Exchange E-mail platform, when a mailbox reaches 49GB, a user will be warned that they are reaching mailbox capacity. At 49GB, a user will be prohibited from sending mail. At 50GB, a user will be prohibited from sending and receiving mail. This setting is controlled by Microsoft and cannot be changed.
Malware	Malware, short for malicious software, is software designed to infiltrate or damage a computer system without the owner's informed consent. Malware represents a variety of hostile, intrusive, or annoying software or program code.
Message Size Limits	<p>In GroupWise, the default message size limit is 10MB.</p> <p>After the migration to Microsoft Exchange, the maximum message size limit will be 25MB. This setting is controlled by Microsoft and cannot be changed.</p> <p>E-mail on both GroupWise and Microsoft Exchange is not intended to serve as a file transfer mechanism for large files (i.e. files over 10MB).</p>
Personal E-mail Accounts	Non-County E-mail accounts held by or available to County Workforce Members for personal or other use, or non-County E-mail accounts of vendors, business associates, or other persons who are not Workforce Members.
Phishing	In computing, phishing is a criminally fraudulent form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as usernames, passwords, and credit card details. Phishing attacks are fraudulent electronic communications, such as an E-mail or an instant message, that purport to be an official correspondence from a trustworthy source. The term phishing arises from the use of increasingly sophisticated lures to "fish" for users' confidential financial information including passwords and bank details.
SPAM	E-mail that is not requested. Also known as unsolicited commercial E-mail (UCE), "unsolicited bulk E-mail" (UBE), "gray mail" and "junk mail." SPAM is used to advertise products or to broadcast political or social commentary.
Users	Synonymous with Workforce Member



Workforce Member	As used here, workforce members include all County employees as well as temporary workers, contractors, consultants, vendors, volunteers, business affiliates or other persons who may, during their association with the County, operate computer equipment on behalf of the County or operate computer equipment that remotely accesses the County's internal network.
------------------	--

## 8. Revision History

Effective Date
April 16, 1999
March 24, 2003
April 28, 2003
March 26, 2007
March 26, 2015