COUNTY OF SAN DIEGO
Health and Human Services Agency

LIVE WELL SAN DIEGO

## N - 01: County Email Use

**POLICY:** See HHSA-N-01 County Email Use, at www.cosdcompliance.org.

**DEFINITIONS:** See HHSA Policy N-13 Security Definitions.

**PROCEDURES:**

1. Authorized Use of County Email
    a. County email accounts are intended for official County-related work, including job duties, program communications, and coordination with internal or external partners.
    b. County email accounts are County property and users have no expectation of privacy.
        i. All activity may be monitored and subject to audit, records requests, or investigations.
2. Personal Use
    a. Limited personal use is permitted if it:
        i. Is reasonable and infrequent,
        ii. Does not interfere with work duties, and
        iii. Complies with this procedure and applicable policies.
3. Prohibited use
    a. County email and systems may not be used for the following activities:
        i. Personal or Non-County Communications
            a. Sending non-business content such as jokes, memes, chain letters, or bulletins.
            b. Using County email to express personal views (religious, political, social) in a way that implies County endorsement or disrupts business operations.
            c. Conducting personal business or side ventures (e.g., real estate, product sales).
            d. Accessing personal email accounts (e.g., Gmail, Yahoo) without written approval.
            e. Using unapproved messaging apps (e.g., WhatsApp) on County devices or for County business.
            f. Using County email to subscribe to or register for third-party services or applications without an authorized business need (e.g., AI tools, external platforms, or mailing lists).
        ii. Inappropriate or Offensive Conduct
            a. Sending or forwarding messages that are obscene, threatening, harassing, pornographic, or discriminatory (e.g., slurs, sexual content).
            b. Bullying or cyber-harassment via County systems.

iii. Security & Privacy Violations
    a. Forwarding County emails to personal accounts or saving to unauthorized storage devices.
    b. Sharing protected information (e.g., PHI, PII) without proper safeguards (e.g., encryption).
    c. Responding to external or unsecure emails containing sensitive data instead of initiating a secure message.
iv. Account misuse
    a. Using another employee's email account without authorization.
    b. Sharing login credentials or sending on behalf of others without formal delegation.

b. Suspected misuse of email – including harassment, discrimination, or ethics violations – should be reported to your supervisor or the Office of Ethics and Compliance (OEC).

4. Handling Protected Information (PHI/PII/Other Sensitive Data)
    a. When emailing Protected Information
        i. Verify Recipients Carefully
            a. Do not solely rely on autofill when entering recipient addresses.
            b. Do not place sensitive information in subject lines as this information cannot be encrypted.
        ii. County-managed mobile devices (e.g., iPhone, Android) cannot encrypt email through the Outlook app. To send protected data securely on mobile devices:
            a. Use Outlook via Microsoft Office Web via a browser, or
            b. The sender is on the HHSA Mandatory Email Encryption list, or
            c. All email recipients are on the vetted HHSA TLS Business Partner list.
        iii. Limit Distribution
            a. Share only with those who are authorized and need the information.
            b. Share only the information necessary for the recipient's role or task. Avoid including full documents or unnecessary details when a brief summary or specific excerpt is sufficient.
    b. External Emails with Sensitive Information
        i. Review and Respond to Sensitive Email Threads Carefully
            a. You are responsible for the entire email conversation thread.
            b. Before replying, review the full thread and remove or redact any sensitive information that is not necessary – especially when adding new recipients.
            c. If you receive an unencrypted email containing protected information (e.g., PHI or PII), do not reply directly. Instead, start a new message using a County-approved secure method (e.g., encrypted email, phone, or in person).

**ⓘ Exception – Individual Request for Unencrypted Communication**

- In limited cases, an individual may request their own personal information be sent unencrypted. This must be documented using HHSA Form 23-05, acknowledging that they understand and accept the risks.

- Third parties (e.g., attorneys, representatives) may not request unencrypted delivery on someone else's behalf.
- For more detailed guidance, refer to *HHSA Procedure L-05: Client Requests for Confidential/Alternative Communications*.

b. Outlook and Team Calendar Invites

Calendar invitations sent via Outlook or Microsoft Teams cannot be encrypted. Do not include PI (e.g., full client names, case numbers, demographic or health information, or other sensitive details) in calendar invites sent outside the County.

i. Use first names, initials, or generic appointment labels when scheduling meeting with clients or external parties.

c. Email Signature & Confidentiality Notice

i. Use the approved HHSA/ Live Well San Diego email signature at the bottom of all messages per HHSA branding guidelines.

ii. Refer to HHSA branding resources or consult your supervisor for a department-approved email signature template.

a. Confidentiality Notice (Optional)

i. While not required, it is recommended to include a confidentiality notice when emailing third parties outside the County network and the message contains protected information (e.g. PHI or PII).

ii. Sample Notice:

a. CONFIDENTIALITY NOTICE: This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain information protected by applicable laws and regulations. If you are not the intended recipient, you may not review, use, copy, disclose, or distribute this message or its attachments. Please notify the sender and delete the message and all attachments immediately.

b. Including the notice does not replace the need for encryption or recipient verification.

c. The notice does not create attorney-client privilege.

2. Security and Phishing Awareness

a. Do not open, reply to, forward, or click links or attachments from unknown or suspicious senders. Avoid downloading files or enabling macros in a suspicious email.

b. Watch for email spoofing. Review sender addresses for subtle misspellings or impersonations of County partners.

c. Report suspicious emails using the Phish Alert Button in Outlook to notify IT Security.

d. If you are unsure whether an email is legitimate, contact your supervisor before responding.

3. Retention

a. Emails older than 57 days in your Inbox, Drafts, and Sent folders are automatically moved to the "Deleted" folder.

b. After 60 days, deleted emails are permanently removed from the system and cannot be recovered.

a. To retain beyond 60 days, save them to a secure, County-approved location.
    i. Do not store emails containing Protected Health Information (PHI) on SharePoint Online, OneDrive, or Microsoft Teams. These platforms are not approved for HIPAA-covered information.
    ii. If you are unsure whether the content qualifies as PHI or whether a storage location is approved for PHI, consult internal guidance or your supervisor before storing the email.
b. Emails are considered public records under the Public Records Act (PRA), but not all emails qualify as "official records" requiring long-term retention. County employees are responsible for preserving any email that meets the official record criteria, based on the applicable retention schedule. If unsure, contact your supervisor.

2. Notice on Email Monitoring and Enforcement
    a. County email accounts are County property, and users have no expectation of privacy.
        i. All email activity may be logged, monitored, or reviewed, and is subject to records requests, audits, or investigations
    b. Violations of this procedure may result in disciplinary action, including referral to Agency Human Resources and/or legal review.
3. Additional Guidance
    a. Employees should also reference the *County of San Diego Administrative Manual Item 0040-11* for additional direction on email use, including:
        i. Identifying and preserving official records
        ii. Responding to public record requests
        iii. Avoiding cyber harassment
        iv. Using secure voice or voicemail communication
    b. If you are unsure about email retention or how to respond to public records requests, consult with your supervisor.

**QUESTIONS/INFORMATION:** Please contact HHSA Business Assurance and Compliance (BAC) by email at Compliance.HHSA@SDCounty.ca.gov or by phone (619) 237-8571.