

Email Use Procedures

The standard email system for SDCOE is Microsoft Exchange (the “SYSTEM”). Official communications are transmitted to employees via the SYSTEM, especially from Human Resources and the Superintendent’s office. The proper and acceptable use of the SYSTEM shall be maintained at all times. The SYSTEM exists for the purpose of providing written communication between SDCOE staff and its stakeholders and is a primary means of disseminating important information within the organization.

This document defines eligibility to possess an account to use the SYSTEM, procedures for requesting a new account, acceptable use, proper etiquette, account expiration, ownership of data within the SYSTEM, associated password policies, privacy, spam, document archival and the use of outside email systems

1. Eligibility

All regular, active, permanent employees are eligible for email accounts on the SDCOE email system (the system). Regular employees are assigned to budgeted positions, governed by bargaining unit contracts and/or Personnel Commission rules. They may be full or part-time. Accounts for the SYSTEM accounts are established via the SDCOE Windows active directory system when a new employee is hired. The use of the SYSTEM is a privilege and is subject to the terms and conditions set forth in this regulation.

Temporary Employees supplement the Regular employee workforce and are also eligible for restricted email accounts on the SYSTEM. Temporary Employees are sometimes referred to as Limited Term, Substitute, Extra Help or Consultants. These are at-will employees and are called on to work as needed. They are not governed by any contract language and SDCOE is not obligated to offer work or on-going employment. Their use of the SYSTEM is restricted to the duration of their work assignment.

Outside agents who perform services under a Performance Agreement are generally not eligible for accounts on the SYSTEM.

Exceptions: Requests for accounts for individuals who do not meet the stated eligibility criteria must be made to the Assistant Superintendent, Integrated Technology Services. Requests will be evaluated weighing the business need versus the associated risk presented in each case.

2. New System Account

Human Resources notifies ITS (Network Services and the User Support Services Help Desk) of all personnel transactions. These include ad hoc notifications for each new hire when processed by HR. The notices include the employee name, start date, the department and division as well as the immediate supervisor.

Network Services creates a new Active Directory account and Exchange mailbox for the new employee. The Help Desk also creates a new service ticket in the employee’s name to establish the initial login to the SYSTEM and ensure proper setup of the employee’s email program.

Exceptions: In cases where a new hire reports prior to the HR notification, the employee’s immediate supervisor should contact the Help Desk to request a new account. The Help Desk will verify the employment status of the new hire and initiate the above procedure.

3. Privacy

The SYSTEM is owned and operated by SDCOE. Email in the SYSTEM may be monitored for content. SDCOE may inspect the contents of any individual or group mailbox. No employee can expect that communication within the SYSTEM is private.

Email should be considered a postcard sent in the public mail. The information is delivered to the addressee but can be read at any time in transit or after delivery.

4. Acceptable Use/Abuse/Etiquette

Respectful, professional communications—including via email—are vital to conducting business and building relationships with colleagues and the general public. It is important that our communications:

- Are respectful in tone
- Are consistent across our employees, programs, and offices
- Comply with SDCOE policies and procedures about confidential information, acceptable use of technology, use of SDCOE resources for political activities, etc.

By ensuring our communications meet these standards, SDCOE employees will convey a professional image, ensure efficient and accurate responses, and prevent misunderstandings and even legal problems. These guidelines have been created to assist employees in ensuring emails rise to these standards.

Using email

- Limit use of SDCOE.net email to official business. Reference Administrative Regulation 3600 for SDCOE policy on acceptable use of technology
- Use a common sense email subject line
- Keep messages brief and to the point
- Always use the spelling and grammar check feature and proofread for errors
- Be considerate of other people's time by not answering emails simply to say "I agree" or "Thanks" unless it is important to let the sender know you received the message
- Use blind copies judiciously
- Do not use email "stationary" or backgrounds
- If you will not be checking your email for longer than one day, set up an "out of office" automatic reply feature

Unacceptable email use

Includes but is not limited to:

- Sending email with content or links that are threatening, obscene, repeated and unwanted, harassing, and/or racially, sexually, or ethnically offensive
- Sending email with content that slanders, libels, or defames anyone
- Sending chain letters
- Sending work-related information to unauthorized recipients
- Sending or receiving software or other products outside of licensing agreements
- Using SDCOE email for personal use (including political, social, religious, recreational, financial gain)
- Unauthorized access of someone else's computer or mailbox
- Revealing confidential information via email
- Using email for illegal or unethical activities

Email signatures

A signature block is a block of text automatically appended at the bottom of an email message. Email signatures contain contact details, including the sender's title and organization name, which help the recipient get in touch. SDCOE staff should use a standard email signature format, customizing information as necessary.

Periodically, SDCOE's Chief Communications Officer (CCO) will email all employees a few sentences to be added to each individual's email signature. These lines are intended to draw attention to SDCOE programs, services or activities in order to increase general awareness.

SDCOE email signature convention

Use a closing signature consisting of your name, title, organization, telephone number, email address, website URL, and the standard signature language for the month (in italics).

Signatures should not include quotes other than the standard email signature provided by the CCO.

Email signatures may include badges associated with SDCOE programs (such as badges earned through Leading Edge Certification). Other badges are not to be used in SDCOE email signatures.

Example:

Firstname Lastname

Title

San Diego County Office of Education

Phone: 858-xxx-xxxx

Email: myemail@sdcoe.net

Web: www.sdcoe.net

School is back in session and San Diego County students continue to make gains on standards-based tests. Learn more about the recent California Standards Tests results at www.sdcoe.net.

Additional resources

Questions regarding email etiquette or email signatures may be directed to the Chief Communications Officer at communications@sdcoe.net or 858-292-3719.

All use of the SYSTEM must also comply with SDCOE Administrative Regulations 3600, "Use of Technology" and 4020 "Code of Ethics."

Any suspected abuse of the SYSTEM should be reported to the Assistant Superintendent, Integrated Technology Services or designee.

5. Account Term/Expiration

Regular Employees: Access to the SYSTEM is available while the employee remains a Regular Employee and is revoked upon resignation, retirement or release from SDCOE

Temporary Employees: Access to the SYSTEM is granted in monthly increments. The immediate supervisor must request extension of all Temporary Employee accounts.

Exceptions: The Assistant Superintendent, Integrated Technology Services may grant a later account expiration, at his/her discretion, to meet the business needs of SDCOE.

6. Continuance of Privileges/Staff Resignations/Terminations

The SYSTEM is a tool provided to current SDCOE employees. Individuals who are no longer employed by SDCOE are not eligible for an account and will have no access after their separation date.

SDCOE will not forward email from the SYSTEM to outside accounts for any separated employee. All email in the SYSTEM is the intellectual property of SDCOE.

7. Data Ownership

All email, files, attachments, calendar entries and task items are the exclusive property of SDCOE. The bulk release of any data from the SYSTEM requires the prior authorization of the Assistant Superintendent, Integrated Technology Services. No data is transferable to any former employee upon separation from SDCOE.

8. Unnamed Group Accounts

Individual employee accounts in the SYSTEM are named and associated with each employee's name. However, there are instances where internal "public folder" accounts may be created to facilitate a department's work flow. Email delivered to these accounts may be accessed by members of the public folder group. A moderator is assigned from each to manage the email items in the folder. Public folders may be requested through the SDCOE User Support Help Desk.

9. Password Policy

An SDCOE email account is a valuable asset that uniquely identifies each employee. Passwords for the SYSTEM are the user's Windows logon password to the SDCOE Active Directory domain. The password used to access the SYSTEM should be kept private to safeguard one's identity and privacy and should not be shared.

The SYSTEM requires a strong password that meets the following criteria:

- It must be a minimum of seven (7) characters;
- It must contain three of the following types of characters:
 - Uppercase letter
 - Lowercase letter
 - Numeral
 - Non-alphanumeric characters (% , ! , & , for example).
- It cannot contain a user's logon name.
- It cannot contain any portion of the user's full name.
- It must be changed every 365 days.
- When changed, it must not match the previous password.

In the event of a locked user account or a lost or forgotten password, staff shall contact the SDCOE User Support Help Desk to request assistance. Employees may be asked to provide additional information to prevent identity theft.

10. Spam

Spam is the use of electronic delivery systems to send unsolicited bulk messages. Spam can cause a reduction in performance of the SYSTEM and can create situations in which the SYSTEM fails completely. Spam is generally associated with advertising but it is also used in criminal activities (phishing) that solicit personal information from people used to steal identities or access personal financial information. In many instances, desktop computers infected with certain viruses are used as launch pads for these phishing attacks. Spam can cause the listing of the SYSTEM in public databases of spammers. Other email systems that subscribe to these lists may block email delivery from the SYSTEM.

Sending spam:

All users of the SYSTEM are prohibited from sending spam under any circumstances. Email should only be sent to individuals with whom SDCOE has an existing relationship and should never be sent unsolicited and to large numbers of recipients. SDCOE utilizes listserves to send out messages to large groups of users who opt-in to receive related communication within their groups.

Receiving spam:

SDCOE utilizes an email gateway product as part of the SYSTEM that analyzes incoming email and classifies it as deliverable or as spam. Spam is quarantined in a 7 day holding area. Users are notified daily that they have received spam and can review these messages. A message improperly classified as spam can be released from the quarantine via a web site.

Spam techniques change frequently as spammers try to defeat anti-spam systems. Users may see a periodic increase in the number of unwanted messages received as these techniques leapfrog the anti-spam methods used in the SYSTEM.

11. Security

All normal communication through the SYSTEM should be considered publicly readable, open and insecure. Messages that traverse the Internet can potentially be viewed by others who are not recipients and should be treated as non-confidential. Email can be considered like a postcard sent in the U.S. Mail.

12. Quotas

At present, the SYSTEM does not enforce quotas governing the maximum size of any mailbox. However, SDCOE reserves the right to impose email storage quotas for any and all accounts on the SYSTEM.

13. Archival

A copy of all email in the SYSTEM is archived upon receipt in a legal compliance mailbox for archival and legal “e-discovery” purposes. Email in the SYSTEM is archived for a period of the prior full 3 years plus the current school year. Some email in the SYSTEM may be archived for longer periods of time as required to comply with local, state and federal requirements. Expired email will be removed from the SYSTEM.

The creation and storage of off-line copies of email is prohibited. All messages in the SYSTEM must comply with the archive requirements.

14. Attachments, Viruses and Malware

The SYSTEM can receive attachments up to twenty-five (25) megabytes in size. Many other systems, however, have much smaller size limits on incoming messages.

The SYSTEM blocks the delivery of files with filename extensions that pose a significant risk to SDCOE systems. These files often hide viruses. These are typically file extensions that end in .zip, .scr, .exe, .pif, .com, .bat, .pi, .uue, .cmd, .vb, .vbs, .is, .elm, .chm, .hta, .wsh, .msi, .b64, .bhx, .hqx, .rar, .mim, .uu, .xxe, .cpl, .jpeg and .png

The SYSTEM scans all incoming email for viruses and other malware threats. However, new threats are discovered hourly and there is no guarantee that every scanned file is truly virus free. Users should not open attachments that are suspicious or unexpected. Many virus infected email is delivered from accounts a user may recognize. Users should attempt to verify with the sender the legitimacy of an unexpected attachment before opening the file(s).

If a user of the SYSTEM inadvertently opens a suspicious file or web site link, the user shall contact the User Support Services Help Desk immediately to report the incident and to initial removal of any infection.

Once reported, harmful email may be deleted by system administrator throughout the entire SYSTEM to preserve the integrity of the SYSTEM.

15. Use of Personal Devices

The SYSTEM is accessible to many wireless communication devices. The use is regulated by SDCOE Administrative Regulation 3513.2, Telephone and Wireless Communication.

An assistant superintendent may authorize access to the SYSTEM on an employee’s personal wireless communication device as part of a work assignment for the conduct of SDCOE business.

Access to the SYSTEM will be provided to an authorized employee under the following conditions:

1. The employee agrees to configure his/her activated wireless communication device(s) to require password access. To maintain SDCOE network security, employees are discouraged from saving passwords in the email configuration of the device.

2. The employee agrees to notify Integrated Technology Services immediately in the event of loss or theft of his/her activated wireless communication device(s).
3. The employee agrees to comply with SDCOE acceptable use, data security policies and all applicable Board Policies, administrative regulations, and state and federal laws. Violations may result in the revocation of access privileges