Central Coast Community Energy

CLEAN ENERGY. LOCAL CONTROL.
3CEnergy.org

IT3
CATEGORY: INFORMATION TECHNOLOGY

E-MAIL USE POLICY

I. PURPOSE

Ensure the proper use of Central Coast Community Energy’s (CCCE) e-mail system and make users aware of what CCCE deems as acceptable and unacceptable use of the e-mail system. This policy outlines the minimum requirements for use of CCCE e-mail.

These guidelines are intended to provide CCCE employees with general examples of acceptable and unacceptable uses of CCCE’s e-mail system.

II. SCOPE

All users of CCCE’s e-mail system.

III. DEFINTIONS

“**E-Mail**” refers to the electronic transmission of information through a mail protocol such as SMTP or IMAP. CCCE’s typical e-mail client is Microsoft Outlook.

“**Chain e-Mail or Letter**” refers to e-mail sent to successive people.

“**Forwarded e-Mail**” refers to an e-mail message resent from an internal network to an outside address.

“**Sensitive Information**” includes all data, in its original and duplicate form, which contains personal information, protected health information, customer record information, card holder data, confidential personal data, or information that is deemed to be confidential or is otherwise exempt from disclosure under state law.

“**Unauthorized Disclosure**” refers to the intentional or unintentional revealing of sensitive information to people, whether inside or outside of CCCE, who do not need to know that information.

“**User**” is anyone using CCCE IT e-mail including, but not limited to: employees, contractors, limited-term employees, and interns.

IV. POLICY

A. BUSINESS PURPOSE

This e-mail policy governs the use of CCCE's e-mail system at any location and using any device, CCCE-provided or other.

All use of e-mail must be consistent with CCCE policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

CCCE e-mail account should be used primarily for CCCE business-related purposes; personal communication is permitted on a limited basis, but non-CCCE related commercial uses are prohibited.

The CCCE e-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any e-mails with this content from any CCCE employee should report the matter to their supervisor immediately.

Employees are prohibited from using CCCE resources to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for a religious or other personal cause.

E-mail signatures, if used, shall only include business-related information such as name, title, CCCE contact information, CCCE logo, links to CCCE websites and/or social media accounts, and CCCE-related messages.

B. PERSONAL E-MAIL ACCOUNTS

Incidental use of CCCE resources (computers, networks, or software) for accessing personal e-mail accounts is acceptable.

Employees may not configure auto-forwarding of CCCE e-mail to external e-mail accounts.

Employees may not use personal e-mail accounts or text messages to conduct official CCCE business.

Users are prohibited from using third-party e-mail systems and storage servers such as Google, etc. to conduct CCCE business, to create or memorialize any binding transactions, or to store or retain e-mail on behalf of CCCE. Such communications and transactions should be conducted through proper channels using CCCE approved documentation.

C. ACCESSING CCCE E-MAIL ON PERSONAL DEVICES

Any employee who connects to or stores CCCE work e-mail on a personal device is responsible for safeguarding access to the CCCE mailbox. Any such device used by the employee must be owned by the employee.

Access to a CCCE e-mail account must always be under user control. The user is responsible for all e-mails sent out from the account whether or not they intended the e-mail to be sent. The user is required to maintain security for the device for as long as CCCE work e-mail is accessible from the device.

In the event the device is lost or stolen, the user is required to change (or arrange to have changed) the e-mail account password and any other account credentials that may be compromised as soon as possible, no more than 24 hours after the discovery of the theft or loss.

CCCE, its employees, directors, and management staff are not liable for loss of personal information, files, etc. stored on user's personal device as a result of access to CCCE's e-mail system.

D. PASSWORDS

E-mail passwords are the property of CCCE. Only specific CCCE approved personnel are authorized to access another employee's e-mail. Misuse of passwords, sharing of passwords with others, and/or the unauthorized use of another user's password will result in disciplinary action, up to and including termination.

E. SENSITIVE DATA

Wherever possible, sensitive data should not be transferred via e-mail as e-mail is not generally encrypted. To minimize the sensitive data loss via e-mail communications, sensitive information should not be included in the body of an e-mail.

Best Practice: It is recommended that sensitive information be transferred in a password protected file attached or linked to the email. When notifying the password to the authorized person for opening that document, the password should not be in the same e-mail with the password protected document.

F. NO EXPECTATION OF PRIVACY

All communications and information that pass through the CCCE IT systems and services, including e-mail, belong to CCCE. The federal Electronic Communications Privacy Act of 1986 gives management the right to access and disclose all user e-mail messages transmitted or received via the organization's IT systems and services. When it comes to e-mail, users should have no expectation of privacy. CCCE reserves the right to access and monitor e-mail at any time for any reason without notice, and may disclose e-mail to regulators, courts, law enforcement agencies, and other third parties without the user's knowledge or consent.

G. OFFENSIVE CONTENT AND HARASSING OR DISCRIMINATORY ACTIVITIES ARE PROHIBITED

Messages containing defamatory, obscene, menacing, threatening, offensive, harassing, or otherwise objectionable and/or inappropriate statements—and/or messages that disclose personal information without authorization—are prohibited. If you receive this type of prohibited, unsolicited message, do not forward it. Notify your supervisor and/or HR Manager about the message.

H. BUSINESS RECORD RETENTION

E-mail messages are written business records and are subject to laws and policies for retaining and destruction of business records. Refer to P&P AD4 - Records Retention Policy for details.

I. PHISHING

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity (e.g. another company or a government agency) in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors, or IT administrators are commonly used to lure unsuspecting users. Phishing e-mails may also contain links to websites that are infected with malware (software that harms your computer or enables extraction of information from your computer). Phishing often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

If you receive any such e-mails that you feel have any suspicious or potentially fraudulent content, do not reply or click on any links on the e-mail and notify IT staff immediately for further instructions.

J. E-MAIL MANAGEMENT, RETENTION, AND ARCHIVING

As a best practice, employees should be aware of the importance of proper e-mail management, retention, and archiving practices, and consider issues including basic individual organization, e-mails as legal records, and physical storage space. Defining a management, retention and archiving policy is a balance of all these considerations. The policy below provides guidelines on the management of e-mail.

E-mails typically fall into two main types – transitory and retainable:

1. **Transitory e-Mails**

   Transitory e-mails do not set policy, establish guidelines or procedures, certify transactions, confirm major decisions, or become a receipt. They convey information of a temporary importance. Examples include:

   - Telephone messages
   - Invitations and responses to invitations
   - Thank you messages
   - Replies to routine questions
   - Spam or unsolicited e-mails

   Transitory e-mails are the most prevalent in our day-to-day work and should be the ones most regularly cleaned up (i.e.. deleted).

2. **Retainable Records**

   E-mails that are informational, related to decision making, received in connection with a transaction, or are otherwise seen as having referable importance in the future may be considered as retainable records. Examples include:

   - Activity reports
   - Audit trail reports
   - Management reports
   - Project work plans
   - Status reports
   - Requests for information or action
   - Statements of policy
   - Documentation of oral exchanges from meetings or telephone calls during which business was discussed, policy formulated, or decisions taken

   Retainable Records should be filed and/or archived according to P&P AD4 – Records Retention Policy.

   Each employee is responsible for managing all sent and received e-mails. This refers to the sorting, filing, and retaining or deleting of e-mails. In general, basic “housekeeping” of e-mails includes:

   - General organization (e.g. use of folders)
   - Periodic purging of personal e-mails (especially those with large attachments)
   - Retention of those that are work related
   - Detaching of large but important attachments to your PC (in both received and sent e-mails)

- Use of the archiving function in your e-mail software (where available)

The larger your e-mail account, the slower it will be and the harder it is to find things. CCCE resources also need to be increased as more and more e-mail data is stored.

V. POLICY COMPLIANCE

A. COMPLIANCE MEASUREMENT

IT staff will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

B. NON-COMPLIANCE

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.