College of the Atlantic Email Policy

Purpose

Electronic Mail is a tool provided by the College and serves as a primary means of communication and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, ethical and lawful manner. Use of College Email Accounts evidences the user's agreement to be bound by this policy. In the event a College employee holds multiple College Email Accounts, the most stringent rules of this policy shall apply.

Account Creation

College Email Accounts are created based on the official name of the staff or faculty member as reflected in the Business Office records. Student and alumni accounts are created based on user ID reflective of the name on file with the Registrar. Requests for name changes to correct a discrepancy between an email account name and official College records will be processed, in which case the email account name will be corrected. This could be due to error or a person legally changing their name. Requests for mail aliases based on name preference, middle name, etc., are evaluated on a case-by-case basis.

Faculty, staff, or departments can request temporary email privileges for users outside of the College. Full time Faculty or Staff requesting these types of accounts will be required to submit user information, rationale for account, expiration date, & sponsor information. Such requests shall be approved by the appropriate Director level manager.

Ownership of Email Data

The College owns all College Email Accounts. Subject to underlying copyright and other intellectual property rights under applicable laws and College policies, the College also owns data transmitted or stored using the College Email Accounts.

Privacy and Right of College Access

While the College will make every attempt to keep email messages secure, privacy is not guaranteed and users should have no general expectation of privacy in email messages sent through College Email Accounts. Under certain circumstances, it may be necessary for COAIT staff or other appropriate College officials to access College Email Accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security or abuse incidents or investigating violations of this or other College policies and violations of Google’s Acceptable Use Policy. COAIT staff or College officials may also require access to a College Email Account in order to continue College business where the College Email Account holder will not or can no longer access the College Email Account for any reason (such as death, disability, illness or separation from the College for a period of time or permanently). Such access will be on an as-needed basis and any email accessed will only be disclosed to individuals who have been properly authorized and have an appropriate need to know or as required by law.

All email users are bound by the appropriate acceptable use policy of both College of the Atlantic and Google.

Google also retains the right to access to the Gmail Accounts for violations of its Acceptable Use Policy. (http://www.google.com/a/help/intl/en/admins/use_policy.html)

Data Purging

Email messages held under Gmail Accounts will be subject to Google's storage and retention policies, which may change from time to time, with or without notice. As of this writing, retention times are unlimited and storage limits are 30GB.

Record Retention

It is the responsibility of employees to preserve College records, including emails or instant messages in particular circumstances:

· Those who have actual knowledge of matters in which it can be reasonably anticipated that a court action will be filed.

· A subpoena has been served or notice of same has been given.

· Records are sought pursuant to an audit or similar pending or possible investigation.

Expiration of Accounts

Individuals may leave the College for a variety of reasons, which gives rise to differing situations regarding the length of email privileges or expiration of accounts. The policy governing those privileges are set forth below. Notwithstanding the guidelines below, the College reserves the right to revoke email privileges at any time.

- **Faculty** – Faculty may keep their email account for 60 days from the end of the last term in which they taught. If such separation is for cause, email privileges may be immediately revoked without notice.
- **Staff** – Staff may keep their email account for 60 days from the end of their last work week. If such separation is for cause, email privileges may be immediately revoked without notice.
- **Students who leave before graduation** – Students who leave the College without completion of their degree or other program may keep their email privileges for one academic term from the last term when they were registered.
- **Expelled students** - If a student is expelled from the College, email privileges will be terminated immediately upon the directive of the Dean of Students Office.
- **Alumni** – Students who have graduated from the College will be permitted to retain their email privileges if their account remains active. All email accounts that are inactive for a period of one year will be removed. Alumni wishing to reconnect with the College can request an account and one may be provided to them.

Appropriate Use and User Responsibility

No data that is classified as Protected shall be stored in or transmitted via email. This includes but is not limited to personally identifiable information, Social Security number, bank account information, tax forms, background checks, sensitive research data, or other Protected Data.

Users who use email communications with persons in other countries should be aware that they may be subject to the laws of those other countries and the rules and policies on others systems and networks. Users are responsible for ascertaining, understanding and complying with the laws, rules, policies, contracts and licenses applicable to their particular uses.

Use of distribution lists or 'reply all' features of email should be carefully considered and only used for legitimate purposes.

In order to prevent the unauthorized use of email accounts, the sharing of passwords is strictly prohibited. Each individual is responsible for his/her account, including the safeguarding of access to the account. All email originating from an account is assumed to have been authored by the account holder, and it is the responsibility of that holder to ensure compliance with these guidelines.

Inappropriate Use

With respect to College Email Accounts, the exchange of any inappropriate email content outlined below and described elsewhere in this policy, is prohibited. Users receiving such email should immediately contact COAIT, who in certain cases may also inform the Department of Public Safety, The Academic Dean, The Administrative Dean, The Dean of Students or The Office of General Counsel.

The exchange of any email content outlined below is prohibited:

- Generates or facilitates unsolicited bulk email;
- Infringes on another person's copyright, trade or service mark, patent, or other property right or is intended to assist others in defeating those protections;
- Violates, or encourages the violation of, the legal rights of others or federal and state laws;
- Is for any malicious, unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- Intentionally distributes viruses, worms, Trojan horses, malware, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- Constitutes, fosters, or promotes pornography;
- Is excessively violent, incites violence, threatens violence, or contains harassing content;
- Creates a risk to a person's safety or health, creates a risk to public safety or health, compromises national security, or interferes with an investigation by law enforcement;
- Misrepresents the identity of the sender of an email.

Other improper uses of the email system include:

- Using or attempting to use the accounts of others without their permission.
- Collecting or using email addresses, screen names information or other identifiers without the consent of the person identified (including without limitation, phishing, spidering, and harvesting);
- Use of the service to distribute software that covertly gathers or transmits information about an individual;
- Conducting business for profit under the aegis of the College

- Political activities, specifically supporting the nomination of any person for political office or attempting to influence the vote in any election or referendum on behalf of or under the sponsorship of the College.

This list is not intended to be exhaustive but rather to provide some illustrative examples.

Scope

This policy applies to all individuals who use or maintain a College of the Atlantic provisioned email account.

SPAM & Phishing

All incoming email is scanned for viruses, phishing attacks and SPAM. Suspected messages are blocked from the user's inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus infected messages. It is therefore incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases, viruses or phishing appear to be sent from a friend, coworker, or other legitimate source. Do not click links or open attachments unless the user is sure of the nature of the message. If any doubt exists, the user should contact the Helpdesk at helpdesk@coa.edu

Definitions

SPAM is defined as unsolicited and undesired advertisements for products or services sent to a large distribution of users.

Phishing is defined as the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.