HSU Policies: P16-01 Email Policy

Applies To: Community Faculty Staff Student Printer-friendly version
Month/Year Posted: 01-2016
Policy Number: P16-01
Definition

This document describes the email services provided by Humboldt State University (HSU), and outlines the campus' responsible use policy for HSU faculty, staff, students, volunteers, emeriti, auxiliaries, and others who receive a university-provided email account.

Authority

ICSUAM 8000 – System Wide Information Security Policy

Scope

All persons and departments assigned an HSU email account.

Approved by the University Senate on this date: -- September 15, 2014

Approved by the President of Humboldt State University on this date: January 4, 2016

I. POLICY STATEMENT

HSU recognizes email systems as tools for conducting official university business. As such, HSU provides centrally managed enterprise email accounts for faculty, staff, matriculated students and others (as described in this document's Eligibility section).

II. EMAIL USAGE

A. TYPES OF EMAIL USER ACCOUNTS

Individual Employee Accounts

Email accounts for faculty, staff, and others will be created based on user eligibility (see Eligibility section below). The email account generated will be considered the individual's primary email account to be used for official university communication.

Student Accounts

Student email accounts will be created based on user eligibility (see Eligibility section below). The student email account will be used for official university communication.

Shared Accounts

Shared accounts can be created for a department or college to support business operations. Each department is responsible for managing the security and appropriate use of its shared accounts.

B. EMAIL USAGE RESPONSIBILITIES

1. Faculty and staff will use the campus-provided email system when they conduct HSU academic and administrative business.

2. Campus email accounts can be used for incidental personal usage, but all contents of the email system are subject to public records disclosures and subpoena as dictated by local, state, and federal laws.

3. Faculty, staff and other account holders should not send Level 1 confidential information on email. Confidential information includes, but is not limited to, an individual's name in combination with Social Security Number, driver's license/California identification card number, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Level 2 FERPA information is allowed on core Google services, including campus Gmail accounts, due to the CSU Google Contract. Data levels are defined in the Data Classification Standards.

4. Email account holders are responsible for safeguarding access to their campus email when using any computing device.

5. Access to faculty and staff email is provided through a standard set of campus-approved email clients and protocols to ensure consistent and secure service and technical support to email users. (See Faculty and Staff Email Clients and Protocols section below.)

6. Campus email systems can be synced with mobile devices, as defined by the ITS web site.

C. SECURITY AND PRIVACY OF EMAIL

1. Electronic communications such as email content and attachments are university records. As such they may be subject to disclosure in accordance with valid subpoenas, warrants, Public Records Access requests, and other state and federal laws.

2. Email sent to or from campus email systems are property of the university and thus subject to university controls, including elimination, in order to protect network performance and ensure fair use of computing resources.

3. Campus email is scanned and filtered for security threats such as malware, viruses and potentially dangerous files

4. Sections 3 and 5 of the CSU Responsible Use Policy defines scenarios in which the campus may need to access data in individual accounts:

D. PROHIBITED EMAIL ACCOUNT ACTIVITIES

HSU prohibits certain email activities, including the following:

1. Email "masquerading", which misrepresents an email user's account name or host name on a sent email.

2. Automatic forwarding of email from a @humboldt.edu address to a non-@humboldt.edu address by employees. (Users can forward selected, individual emails from a @humboldt.edu address, however auto-forwarding all campus email to non-HSU email accounts prevents HSU from providing email records to legal entities when officially required to do so.)

3. Sending blanket, all-campus email to employees or students except as provided in EM P06-02, Critical Immediate Send Messages and EM P##-## Associated Students Constituent Email Messages ~~(see Critical Immediate Send Messages, EM P06-02 which specifies who can grant exceptions and under what circumstances)~~. This prohibition is not meant in any way to abrogate the rights set out in Collective Bargaining Agreements for unions to utilize university email for union business.

4. Harassment, illegal activities, commercial business, or business.

5. Harvesting directory information.

E. ELIGIBILITY

The following users are provided HSU email accounts, as long as the accounts remain active (defined as accessing the account at least once a year and not allowing the password to expire):

1. Faculty, staff, and volunteers with records created in CMS are eligible for individual employee accounts.

2. Matriculated students are eligible for student accounts.

3. Self-support and auxiliary employees as identified by each auxiliary organization (Sponsored Programs Foundation, Advancement Foundation, University Center, Associated Students, Inc.) are eligible for individual employee accounts.

4. Emeritus faculty and retiring staff as identified by Faculty Affairs and/or Human Resources, as appropriate, may retain their individual employee accounts as long as their accounts remain active.

5. Guests and other individuals may receive email accounts for a limited time by request of campus-defined sponsors by requesting a contractor account.

6. Former students can retain email accounts as long as their user accounts remain active.

7. Individuals eligible for an account who have allowed their accounts to expire can request that a new account be created. This will be done using the same HSU Username, but may have a different email address or alias(es).

F. EMAIL ACCOUNT NAMING CONVENTIONS

1. Each faculty, staff, auxiliary, and volunteer email user is entitled to one mailbox based on their HSU Username (abc123) and a formal alias which is provided per the following naming convention:

   i. firstname.lastname@humboldt.edu

2. When multiple identical firstname.lastname situations occur for email users, uniqueness will be achieved by applying sequential numbering to the email account name or inclusion of middle initials.

3. Each student user is entitled to one mailbox which is provided per the following naming convention:

   i. HSUUsername@humboldt.edu

4. Student aliases and additional employee aliases are available through Account Settings on request.

5. HSU reserves the right to transition former students and retired employees to alternate email addresses (e.g., @alumni.humboldt.edu or @emeritus.humboldt.edu) at some point in the future.

G. TERMINATION OF EMAIL ACCOUNTS

An email account will be terminated following due process. Typical termination conditions are:

1. Standard employment separation, termination, or retirement:

Users who do not have a current faculty, staff, emeritus, volunteer, alumni, or auxiliary status in Peoplesoft will have their account terminated.

For a limited period of time, faculty member accounts may be retained by the university and may be accessed by a separated, terminated, or retired faculty member to address grade appeals.

2. Violation of Campus Computing Policies or Guidelines:

Violations as defined in the campus acceptable use policy or campus computer usage and safety guidelines will result in email account termination.

3. Disciplinary Action:

The account will be handled based on direction from Student Conduct, Human Resources, Faculty Affairs or University Police. This will generally involve suspending, deleting or reassigning the account.

4. Inactivity:

If an account is not accessed for a year, or if the password is allowed to expire, it will be considered inactive and may be suspended, archived, or deleted.

H. FACULTY AND STAFF EMAIL MESSAGE RECOVERY

1. Email Message Recovery

Email messages deleted by a user are automatically emptied from the user account's trash bin on a periodic basis and may be manually emptied from the trash bin anytime by the user. After automatic removal, which Gmail currently does after 30 days, or manual removal from an account's trash bin, a message should be assumed to be irretrievable.

2. Email Message Archiving

Email message archiving is not provided because there is ample inbox and folder storage available.

I. EMAIL STORAGE AND MESSAGE SIZES

The email system provides at least 25 gigabytes of email storage to faculty, staff and students.

Google currently allows messages up to 25 megabytes in size (including attachments) to be sent and received.

J. FACULTY AND STAFF EMAIL CLIENTS AND PROTOCOLS

The email system can be accessed using standard campus-approved email clients and protocols as defined by the ITS web site

K. USING CAMPUS EMAIL WITH MOBILE DEVICES

Mobile device operating systems that have been tested and are recommended for use are listed on the ITS Email Services page.

Personal mobile devices can be configured by users to synchronize with the HSU email system and instructions are available for the recommended mobile devices.

L. EMAIL RETENTION

Email, by itself, is not specifically listed as a 'record type' within the CSU records retention and disposition schedule. An email may become a record depending on its content. If an email is deemed a record then it is subject to the CSU retention and disposition schedule and should be moved to more permanent storage. Refer to the CSU Records Retention and Disposition Schedules.

IV. RESPONSE TO VIOLATIONS

The University reserves the right to temporarily or permanently suspend, block, or restrict access to information assets when it reasonably appears necessary to do so to protect the confidentiality, integrity, availability, or functionality of those assets.

Any disciplinary action resulting from violations of these guidelines or program supporting policies, standards or procedures shall be administered in a manner consistent with the terms of the applicable collective bargaining agreement and/or the applicable provisions of the California Education Code.