Technology Policies and Procedures
Eureka College

This document contains current technology-related practices and procedures associated with Eureka College Network (ECNet) including additional information on Email, G Suite for Education (formerly Google Apps for Education), and Wireless Access.

Eureka College (EC) IT Services provide technical assistance for technology services provided by the College and maintain campus-owned technology-related equipment. EC reserves the right to restrict types of devices that can be connected to the ECNet. Users may connect their personal devices to the ECNet after going through a device registration process. No self-provided wireless services or networking equipment are allowed on ECNet.

For more information on IT policies and other ECNet services including account deactivation, visit the policy section of the IT website (it.eureka.edu), or appropriate sections of EC website and Handbooks. Users may also contact the IT Staff for any assistance with IT Policy-related matters.

Assignment of User Accounts

Student applicants with an enrollment deposit will be issued an email account and other necessary login accounts. Upon employment, Faculty and Staff will be assigned ECNet and other necessary accounts when the Human Resources Office sends a request to IT Services (via helpdesk@eureka.edu) and additional access is assigned as the appropriate administrative unit submits a written request.

All login accounts issued to an individual are intended for the sole use of that individual and are non-transferrable. The owner of the account is responsible for all network activities on that account including activities via registered personal devices on ECNet. It is not acceptable for a user to share any login account, to share its password, or to use accounts of other users.

Users are encouraged to use strong passwords consisting of a mix of lower and upper case letters, digits, and special characters. A minimum password length of 8 characters is recommended. Please do not use dictionary words, easily identifiable personal data, or passwords that can easily be guessed. The users are responsible for protecting their own accounts.

When You Separate from Eureka College

Network accounts for students will generally be deleted fifteen (15) days after separation or graduation from Eureka College. For faculty and staff, ECNet and other administrative accounts will generally be deleted or disabled seven (7) days after separation from EC. The College

reserves the right to delete or disable accounts at any time. EC is not responsible for moving or exporting any personal data from any EC account.

Your G Suite (Google Apps) account is subject to the following conditions:

- For withdrawn students, the email account will be deleted fifteen (15) days after separation from the academic program.
- For EC graduates, your email account will remain active after graduation, but will be removed from the global address book.
- For those faculty members granted faculty emeritus status, please reference the faculty handbook.
- For other faculty/staff;
  - Upon retirement, you may request your email account to remain active. The President's Council will review the request and either approve or deny the request.
  - Upon termination of employment at EC, your email account will generally be deleted seven (7) days after termination of the appointment at EC. The College reserves the right to delete or disable accounts at any time.
- Any email account that is inactive for more than three (3) months is subject to deletion from the email system.

Network and other accounts

- For withdrawn students, network accounts will be deleted after fifteen (15) days of exit based on the information available in the Student Information System (SONIS).
- For Faculty and Staff, network and other related accounts will be disabled or deleted based on the information provided by the Offices of the Provost and Human Resources regarding faculty and staff separation or resignation.

Data Security and Network Shares

User assigned network shares must be used for any important institutional data. Users should not save their own personal data (ex. vacation photos, games) or unknown files on any network share. The College reserves the right to restrict space and access rights on network shares.

The College uses necessary security measures to protect data with sensitive information. Users are also expected to use sensitive information in a responsible manner. For example, email or free online services are not appropriate for sensitive information. Any unknown or user-owned programs or applications are not allowed on campus-owned computers. Users may contact EC IT Services to discuss any data security concerns or to report any potential data-related issues.

Copier/Printer Usage

Students may use printers available in computer labs for their copy/print needs. At the beginning of each semester, each student is assigned a copy/print quota as a monetary value. The fall and spring quota is equivalent to 300 single black and white pages at the current single side cost.

The summer quota is equal to 150 pages. Double-sided copying/printing is considered as two pages. Color copying/printing is five times more expensive than black and white copying/printing. Copying/printing in excess of these quotas will result in an extra cost for students, and this charge will be added to the student's bill. Students have options to monitor their copying/printing costs.

For faculty and staff, the actual copy/print costs are charged as a departmental expense at the end of each billing cycle.

Email and G Suite (formerly Google Apps) for Education Guidelines

Your G Suite (Google Apps) account, which includes your email account, is generally assigned to you with your ECNet login account and is subject to the same privileges, restrictions, and penalties outlined in the ECNet Acceptable Use Agreement.

Adherence to these guidelines is intended to prevent tarnishing the public image of EC. The general public and the EC community tend to view any email messages with eureka.edu domain as an official statement from the College.

Even though EC IT Services manage user accounts associated with G Suite (Google Apps) for Education for EC, all data are stored on Google servers and subject to Google's privacy policies. Users must accept the Google Privacy Policy when activating the account for the first time. EC reserves the right to disable or remove any inappropriate, orphaned, or abandoned G Suite (Google Apps) components from the system.

System Information

EC utilizes G Suite (formerly Google Apps) for Education as our campus email system. Additionally, EC reserves the right to enable only selected additional services, as appropriate, to support its mission. All email accounts are subject to policies applicable to G Suite for Education and EC. Users are expected to manage their email quota and use other selected applications in a responsible manner to support the mission of the College. The Google Groups and other applications under the eureka.edu domain in G Suite for Education should only be used for Eureka College academic and Eureka College business related activities.

Users are expected to use a personal Google account or any other email account for their personal activities. EC is not responsible for moving or exporting personal data from an EC G Suite account (including EC assigned email account).

G Suite Modules

The following modules have been approved by EC for institutional use. Requests for additional services/apps need to be submitted to the IT Advisory Committee.

Google Sites

All Google Sites content must adhere to College policy. It is the site owner's responsibility to maintain and update site content and to adhere to all copyrights of corporate images and external content. If you discover inappropriate or out of date content, contact the site owner directly to discuss the issue. If the problem persists, send a message to helpdesk@eureka.edu.

Google Hangouts

This feature supports voice and video conversations and is available for most EC users. Common courtesy should be extended to all communications.

Google Groups

Faculty, Staff, and Students have the ability to create distribution lists in the system, and the name of the group will end in "-private@eureka.edu." The creator/owner must manage the group and is responsible for all activities associated with that group.

Your EC-assigned email account comes with a subscription to the appropriate group to which you belong: student/staff/faculty (see Campus-wide Distribution Lists below). This email account will be considered your official EC email address. Do NOT unsubscribe from these official groups in order to receive official email communications from the College. Eureka College is not responsible for your subscriptions to other private Google Groups. Please contact helpdesk@eureka.edu if you are not receiving emails intended for you.

Google Docs and Google Drive

With Google Docs, one can create a document and share and edit with others online. Google Drive provides file backup on Google storage systems.

Files and documents should **not** contain sensitive information (Ex. individuals' social security number, credit card information, birth date, unpublished addresses and phone numbers). Be selective when sharing documents with Google Docs and Google Drive.

Google Docs and Google Drive are not to be considered a permanent storage for record retention or archiving purposes. All important documents should be kept on a College maintained network folder for record retention and/or archiving.

Faculty and Staff should retain ownership of their documents within Google Docs when shared them with students. If a student or alum is the owner of a document that a faculty or staff member uses, and that account is removed, then the document will permanently be deleted.

When a faculty, staff or student separates from EC, the College reserves the right to migrate any Google Docs document that the faculty, staff, or student owns to another user at the College.

Campus-wide Distribution Lists

There are system-wide email distribution lists (Google Groups) available for intra-campus communications. Use of these lists is limited to communication necessary to support normal

academic and administrative operations of EC. System-wide email distribution lists should only be used for critical and timely information concerning EC. Organizations, committees and other working groups can create and manage private mailing lists (Google Groups) which include their group members.

1. Faculty and staff authorized by the Provost or the CFO shall have access to the system-wide email lists based on their specific roles and job related duties. They should use these system-wide email lists only for their specific work-related communications. Personal or other types of mass emails should not be distributed via system-wide email lists.
2. Faculty and staff members may request approval for any communication of campus-wide interest as follows:
- On academic matters: send your request to the Provost
- On business matters: send your request to the CFO
- On all other matters: send your request to the VP of Institutional Advancement

If approved, the requested communication will be distributed.

Email communications **not** suitable via system-wide email lists include, but are not limited to
- Messages intended for a small fraction of the email list
- Chain email (any email asking others to forward or re-send the received email)
- Buying/selling personal items
- Trips/events not sponsored by EC or its administrative/academic units
- Commercial advertisements of any type
- Any communications not related to duties associated with the faculty/staff/student member's position at EC

Mass email distributions or email schemes that can disrupt other network services or email servers are prohibited. Private email lists should not be used to cause excessive network traffic or other email disruptions. All community members/organizations are encouraged to compile and use private mailing lists as appropriate.

Common courtesy should be extended to all communications. Fraudulent, harassing, threatening, and obscene messages are not acceptable on the ECNet. Communications associated with personal financial gains shall not be permitted.

If a user sends emails to a group of email recipients at regular intervals (ex. daily or weekly), recipients should have a way to subscribe/unsubscribe to these frequent email communications. The sender is responsible for managing this task. The Faculty, Staff, and Students email lists (Google Groups) under the eureka.edu domain should not be used for this type of regular email communications.

Departments and Organizations Requesting Accounts

A written communication from the VP overseeing the department or organization is required to establish a common departmental or organizational email account. Any unused departmental or organizational email account is subject to deletion if it is inactive for more than 90 days.

Alumni and Employee Transitions

If a former student of the College becomes an employee, the user will be issued a new eureka.edu email account for business/employee use. The naming convention for the new account will follow the standard for faculty and staff. The user must separate personal and business use of the two active email accounts. When the employee separates from the College, the alum account will remain in the system, and the business/employee user account will be removed per policy.

If an employee of the College becomes alumnus/alumnae while employed, and then separates from the college, the business/employee email account will be removed from the system per policy and a new alum account will be created for the user if desired.

Wireless Access Guidelines

Wireless access is available within all buildings on campus. The goal of these procedures are to protect EC technology-based resources (such as data, computer systems, networks, databases, etc.) from unauthorized use that could result in loss of information, damage to critical applications, loss of connectivity, and damage to our public image. Therefore, all users employing wireless methods of accessing EC technology resources must adhere to campus-defined processes for doing so, using wireless access points provided by EC.

Mobile Access

EC is committed to providing authorized users with wireless access to the Internet, and selected internal network resources. In order to make this service available to end users, IT Services or its designated agents must install “access points” in and around the premises wherever wireless access to the ECNet is designated.

- Students and employees must register their mobile devices before using them via wireless technologies available at EC. The registered user is responsible for any activity associated with the registered devices under his or her username.
- Authorized users may register their own mobile devices, but they should not share the passwords or register mobile devices for others.
- EC IT Services sets a limit on the maximum number of registered mobile devices per user based on resources available.
- Guest access is available upon request, with at least 24 hours advanced notice, from an EC employee or student (sponsor), for a limited duration for users identified as EC guests. The sponsor is responsible for any activities of the guest(s) on the campus network.

- A Rogue device is anything with wireless capability and installed without the knowledge or permission of EC IT Services; used by internal or external users to gain unauthorized access to the ECNet and the Internet. Rogue devices are prohibited on the ECNet.
- All wireless access points connected to the ECNet will be centrally managed by EC IT Services and will utilize authentication, authorization, and other security methods at its discretion. Non-sanctioned installations of wireless equipment, and use of unauthorized equipment within the EC campus, are strictly forbidden.
- All access point broadcast frequencies and channels shall be set and maintained by EC IT Services. Any device or equipment found to be interfering with wireless signals may be subject to relocation or removal, including wireless printers, cordless phones, microwave ovens, cameras, any other user-owned equipment, etc.
- The EC IT Services may conduct sweeps of the wireless network to ensure there are no unauthorized devices present on the ECNet.
- The EC IT Services reserves the right to turn off, without notice, any device connected to the network that may cause EC computer systems, data, users, and ECNet resources at risk.
- Users are expected to report to the EC IT Services any incident or suspected incidents of unauthorized device installation and/or disclosure of campus resources, databases, networks, and any other related components of the organization's technology infrastructure.

[Updated in December 2016 and approved by President's Council on December 21, 2016]