Eureka College Network (ECNet)
Acceptable Use Policy

Introduction

This policy, referred to as **ECNet Acceptable Use Policy**, contains general guidelines applicable to all technology-related services provided by the Eureka College Network (ECNet), including, but not limited to, wireless services provided by Eureka College (EC). All students, faculty, staff, and other EC agents or guests receiving any ECNet service constitutes acceptance of this policy.

This policy and other Information Technology (IT) policies and procedures are included in the employee and student handbooks as well as on the IT web site, http://it.eureka.edu. The ultimate responsibility for any policy violation lies with the user who originates such a violation. When a personal device is involved, user is defined as the registered user associated with the device.

Mission Statement

The purpose of the ECNet is to facilitate the exchange of information that furthers the instructional, scholastic, and service goals and mission of EC in a secure networking environment. In support of this purpose, EC requires its faculty, students, staff, and guests to practice behavior that is ethical, responsible, and legal in their use of the network and its services.

Scope

This policy applies to all EC students, employees, guests, and other EC agents who have any device connected to ECNet, including, but not limited to, desktop or laptop computers, mobile devices, and any other device that is capable of network access. This policy covers campus-owned devices as well as any personal devices that connect to the ECNet. For a personal device, the registered user is the owner of that device and the user responsible for any policy violation.

Device Registration

All personal devices connected to the ECNet must be registered. Users may need to install a registration agent on their personal device during the registration process. EC reserves the right to limit types of devices that can connect to the ECNet as well as the maximum number of devices allowed per user. Devices that can interfere with services provided by the ECNet are not allowed. The registered user is responsible for any policy violations associated with the registered device.

Security

EC reserves the right to use appropriate security measures to protect the ECNet and connected devices and users. Devices with security risks are blocked or removed from the network

immediately.

Users are responsible for respecting the security policies of the ECNet and all connected networks, and they are responsible for applying available security measures for protecting their connected devices. (e.g., Users are responsible for applying security patches and anti-virus updates on their personal devices connected to the ECNet; users should select passwords that cannot be easily surmised). Users are expected to take all reasonable steps to insure the integrity, authenticity, and security of the information that they compile or use.

For network and application access, users need passwords. Password requirements can vary by application. These passwords typically meet certain requirements (minimum 8 characters, a mix of uppercase, lower-case, special characters, etc.) with forced password changes at regular intervals. Users are encouraged to change passwords more frequently, as needed.

Acts that disrupt the operation of the ECNet or any connected network are prohibited. Such acts include, but are not limited to, the propagation of computer malware such as viruses and spyware, and transmission of information that degrades the performance, functionality, or reliability of any system. In order to maintain system operations, it may be necessary for the system administrators to monitor account and system activities, and to maintain activity log files. The network hardware, software, and any other user-assigned devices along with IT resources are the College's property and users must treat them as such.

Unacceptable Use

Users are expected to respect the values, individuality, productivity, and rights of other network users. Activities that interfere with this standard constitute a violation of this policy. These activities include, but are not limited to:

- vandalizing data of another user
- impersonating another user
- posting personal communications without consent of the author
- distributing unsolicited advertising or recruiting materials for non-educational purposes
- sending chain mail or excessive messages not desired by the recipient
- attempting unauthorized access to other accounts
- intentional disruptions to ECNet or its services
- using ECNet or its resources for any personal gains
- using the network in illegal, wasteful, threatening, harassing, obscene, or prejudicial ways

Email and G Suite (formerly Google Apps) for Education

EC utilizes G Suite (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 current guidelines 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 EC

academic and EC business related activities.

Even though EC IT Services manage email accounts associated with EC, all Google services are hosted by Google and subject to Google's privacy policies and additional privacy policies as deemed appropriate by EC. Users should not include any sensitive information in emails or store any sensitive information in other areas such as Google Docs, Google Drive, or Google Groups.

Web Pages

EC has an official web site that may link to other web sites and other application-specific web sites maintained by EC. sites.

Copyright and Legal Issues

Web page developers, both official and personal, are responsible for respecting all copyright and trademark rules. Items such as graphics, video, and documents may not be placed on a page without proper consent of the owner of those items.

The College is also required in compliance with the Family Educational Rights and Privacy Act (FERPA). Users with access to sensitive data should take additional precautions when using electronic communications. (Ex. sensitive data should not be sent by email.)

The use of the ECNet to transmit information whose content, meaning, reception, or distribution violates applicable local, state, and federal laws (including export laws) is strictly prohibited.

Network Use and Resource Management

Some network services such as streaming video, peer-peer networking, and distribution of very large data files can cause network disruptions due to excessive use of network bandwidth. EC reserves the right to restrict non-essential applications such as online game playing, peer-peer networking, music sharing, and to manage the Internet bandwidth in support of essential services related to its mission. The use of any networking device that could interfere with the campus network is also a serious policy violation.

Misuse of Network Devices and Resources

Institutionally owned network devices and resources are College property. Misuses and physical equipment damages are handled according to established policies included in employee and student handbooks.

Penalties for Policy Violations

Investigations of policy violations will be handled through the following channels:
Faculty - Chief Academic Officer
Staff - Chief Financial Officer
Students - Judicial Committee

If a violation is viewed as excessive (e.g. email or network disruptions), illegal (e.g. threats,

harassment, spreading malware), or any other network activity that is disruptive to campus or campus network, it may be necessary for the system administrators to immediately suspend the user's connection and/or the account, and inform the Chief Academic Officer, Chief Financial Officer, or Chair of the Judicial Committee with supporting evidence of the connection or account suspension within 24 hours.

Other Related Information

Additional institutional guidelines related to ECNet, G Suite (Google Apps) for Education, and wireless access can be found in the document titled EC Technology Policies and Procedures. All IT-related policies and procedures are included in the employee and student handbooks. These policies are reviewed and updated annually.

Policy Non-Compliance

Failure to comply with the ECNet Acceptable Use Policy may result in the suspension of access privileges, disciplinary action, termination of student status or employment, and possibly legal actions. Please see the EC employee family of handbooks or the student handbooks for details.

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