Security and Acceptable Use of the Campus Network and Technology Policy

The Information Technology Services department, with the oversight of the College's Executive Council, determines the campus network and technology security and acceptable use policy in accordance with the security and preservation needs of Emory & Henry College, best practices in the IT industry, and in compliance with federal, state, and local legal requirements. All students, faculty, staff, and others affiliated with Emory & Henry College receiving a network access account must adhere to the following policies and guidelines. Employment or enrollment at Emory & Henry College signifies agreement to abide by all rules, regulations and policies of the College. Please note that all policies are subject to change. Notification of changes will be posted. This document will be reviewed and published regularly on the College website and in various official College publications such as the Student Handbook, Faculty Handbook and the Staff Handbook. All network users must adhere to the most current published revision.

Guests of the College utilizing Internet access through the College's network are expected to practice good Internet citizenship in their online activities, so as to avoid reflecting negatively on Emory & Henry College. Specifically, they must adhere to all local, state, and federal laws, not download illegally obtained copyright protected materials, and not access websites or materials which are not in keeping with the teaching, research, and educational goals of the institution. Anyone affiliated with Emory & Henry College who allows minor children to utilize public access computers on campus must be responsible for the actions of those children and should remember that Emory & Henry College does not have any filtering hardware or software in place for Internet content. Guests will have limited access to network resources.

All students, faculty, and staff have a network account assigned to them for their individual use while at Emory & Henry College. Emory & Henry College computerized information systems exist to promote shared access to computing, communication, and information necessary to serve the teaching, research, and administrative needs of the entire campus community. These systems and the data they contain are vital resources of considerable monetary and intellectual value, in addition to important personal information which must be handled in a secure and confidential manner. Access to computer systems and networks, including email and web material placed on or distributed through the systems and networks owned or operated by Emory & Henry College is a privilege, not a right, and requires adherence to College policies and federal, state, and local laws. Thus, all account holders of the College's information facilities have a responsibility to use these systems in a respectful, ethical, professional, and legal manner.

The purpose of the network is to support the teaching, research, and administrative needs of the College. The network is not designed nor intended to support the downloading of copyrighted material, such as unlawfully obtained music, videos, and software. Such activities are not permitted at any time. Non-academic online activities, such as gaming and streaming, are allowed, but Emory & Henry cannot guarantee full support of all systems. This policy pertains to all mobile devices, computers, printers, scanners, networks, Internet connections, and communication systems transmitting voice, data, or video information owned or leased by the College or connected to the College network. Appropriate use is always ethical, reflects academic honesty, the security and confidentiality of personal information, and shows restraint in the consumption of shared resources.

All users of Emory & Henry information facilities are required to demonstrate respect for intellectual property, ownership of data, system security mechanisms, and the individual's right to privacy and freedom from intimidation, harassment, and unwarranted annoyance. While recognizing the respect for privacy, the College cannot guarantee confidentiality in the use of any College information system. Electronic records retained on College systems are subject to state and federal Privacy Acts, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), and Commission on Accreditation for Law Enforcement Agencies (CALEA), as well as Freedom of Information Acts. World Wide Web information located in designated web directories will be considered public information if "read" access is granted. Access to and the utilization of data contained within College administrative, academic, and student support administrative systems are also subject to Family Educational Rights and Privacy Act (FERPA) regulations and authorized users agree under this acceptable use policy to adhere to and abide by FERPA privacy and security guidelines. Student and staff medical and counseling records may be subject to Health Insurance Portability and Accountability Act (HIPAA)

regulations and must be accessed and handled in accordance with those established guidelines and regulations. Please note: no confidential data should be stored on any non-Emory & Henry owned and operated file storage solutions, including, but not limited to, third-party cloud storage.

Appropriate Use Guidelines

In making appropriate use of resources Emory & Henry students, faculty, and staff must:

- Be consistent with the purposes of the network. It is designed to support research, education and administrative needs of students, faculty, staff, and administrative personnel.
- Assume responsibility for material on personal web pages.
- Use copyrighted materials only with the proper approval by the copyright holder or in compliance with “Fair Use” guidelines as described in current federal copyright legislation.
- Use resources only for appropriate purposes, such as, but not limited to, assignments given by instructors, college related work, communication. Inappropriate use is described in the section below.
- Discontinue use of a College public-access or lab computer for personal or recreational activities if no other resources are available for students to use for class assignments. Protect the individual’s user logon ID (user account) from unauthorized use. The individual is responsible for all activities on their user ID.
- Access only files and data that belong to the individual user, that are publicly available, or to which the individual user has been given authorized access.
- Use only legal versions of copyrighted software in full compliance with vendor license requirements. Do not make copies of copyrighted software for personal use.
- Be considerate in the use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, bandwidth, or other resources.

In making appropriate use of resources Emory & Henry students, faculty, and staff must NOT:

- Use another person’s user logon ID and password at any time.
- Allow another person other than the actual user to access a user account.
- Use another person’s files or data with permission.
- Use computer programs to decode passwords or access control information.
- Attempt to circumvent or subvert system security measures.
- Engage in any activity that might be harmful to computers or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- Use College systems for partisan political purposes, such as using electronic mail to circulate advertising for political candidates.
- Transmit, distribute, upload, post, or store any material in violation of any applicable law or regulation, or that encourages conduct that could constitute a criminal offense, gives rise to civil liability or otherwise violates any applicable local, state, national or international law or regulation. This includes, without limitation, material protected by copyright, trademark, trade secret or other intellectual property right used without proper authorization.
- Transmit, distribute, upload, post, or store any material that is obscene, defamatory, libelous, unlawful, harassing, abusive, threatening, harmful, vulgar, constitutes an illegal threat, violates export control laws, hate propaganda, fraudulent material or fraudulent activity, or invasive of privacy or publicity rights.
- Use College resources to create personal web pages containing (1)pornography or (2)abusive and/or profane language.
- Place digital photographic or recording equipment of any kind in any public space on campus without the prior written permission of the Dean of Students.
- Waste computing resources, for example, by intentionally placing a program in an endless loop or by printing excessive amounts of paper.
- Use the College’s resources for money making activities as these can jeopardize Emory & Henry’s non-profit status. The network may not be used to advertise a commercial business, or to support a personal business interest. Neither may electronic mail be utilized to circulate advertising for products.
- Engage in any other activity that does not comply with the general principles presented above.
- Peer-to-peer file sharing is now prohibited at Emory & Henry College in compliance with the U.S. Higher Education Act. Downloading movies, music, or other copyrighted materials without permission of the copyright

holder is strictly forbidden. There are numerous legal and legitimate sites in the World Wide Web for the downloading of materials, such as iTunes.com and Rhapsody.com. The College recommends that anyone wishing to download music or other copyrighted materials utilize legal means to do so.
- Any non-computing device must be approved and registered through the IT Help Desk before it can be connected to the network. IT Services reserves the right to restrict devices accessing the network.
- The E&H wireless network does not accept non-College access points. Personal wireless access points, hubs, and routers are strictly forbidden.
- Any Computers connected to the Emory & Henry network are strictly forbidden to function as hosts for network services such as peer-to-peer, file-sharing, local area networks (LAN), etc.

Abuse of Email Privileges

E-mail and network connectivity are a privilege, not a right. These privileges can be revoked for violations of this Acceptable Use policy. Unacceptable behavior includes, but is not limited to:

- Infringement on others' privacy
- Interference with others' work
- Copyright infringement
- Illegal activity
- Use of mass email for commercial or political mailings
- Use of distribution lists for purposes other than teaching, research, and administrative needs of the College
- Penalties for unacceptable behavior range from deactivation of the account through College judicial action or referral to law enforcement authorities. For minor first offenses, the Chief Information Officer/Director of Information Technology will notify the offender with a simple email warning.

Mass Email Guidelines

Mass electronic mailings shall be concise and to the point. The use of attachments should be limited to small size files, such as MS Word and Excel files. Larger files can be posted on the password-protected section of the website or on the learning management system. To post a document on the web site, please contact Public Relations. If you need assistance with the learning management system, please contact the Instructional Technologist. Mass email is recognized as an important medium for facilitating communication within the Emory & Henry community. However, the potential misuse of mass e-mail is also recognized. The policies and procedures found in this document attempts to provide guidance for the appropriate use of the All Employees, All Students, All Users etc. email distribution list.

Remember that the College's official internal electronic newsletter, E&H News, should be used for all general College-related announcements and for providing information about programs, projects and activities. If you need assistance with including these events in the College's electronic calendar, please contact Marketing and Communications. In order to have your news or event featured in E&H News, a request should be submitted to News@ehc.edu by 2 p.m. the day before the announcement should appear in the e-newsletter. If you are unsure about where to post an announcement, please contact the Marketing and Communications for assistance. In addition, discussion forums should be set up through the use of Moodle (not email). If you need assistance with setting up a Moodle account for a discussion forum, contact Valerie Lewis, Instructional Technologist, at vlewis@ehc.edu.

Mass email lists should be used only for the following purposes:

- Instructions from the faculty marshal and/or staff that do not seem appropriate for other communication media.
- Communication from the chair of the staff affairs committee for all faculty and/or staff that does not seem appropriate for other communication media.
- Communication from senior administrators for all faculty and/or staff that does not seem appropriate for other communication media.
- Communication from individual faculty or staff of general interest to a majority of faculty and/or staff that does not seem appropriate for other communication media.
- Distribution of faculty and staff surveys.

- Reports from faculty or staff committees or task forces of general interest to a majority of the faculty and/or staff.
- Reports from the faculty or staff representative to the Board of Trustees.
- Reports from the governance groups (Faculty Advisory Committee, the Staff Affairs Council, etc.).

Urgent Messages

Urgent mass emails are reserved for highly important, time-sensitive emergency notices. In those cases, faculty and staff need to contact one of the following offices and request the message to be distributed to the College-wide community. Urgent messages must be sent in plain text and contain no graphics, bolding, or other HTML formatting. The following is a list of the offices authorized to distribute mass emails to the campus-wide community:

- President's Office
- Provost's Office
- Campus Police/Security
- VP for Business and Finance
- Chaplain's Office
- Centralized Student Assistance
- IT

Urgent messages include the following:

- Messages concerning emergency, health and safety: bomb or terrorist threat; natural disaster alert; mechanical failures; weather closures or delays; crime alerts; and computer virus alerts;
- Health alerts.
- Logistics announcements: construction closures; traffic routing; and ozone or environmental alert notices.
- Messages pertaining to matters of college-wide policy.
- Messages of a timely nature having direct impact on large numbers of faculty, staff, or students.

Web pages on College Servers

The privilege of presenting material on the College web site can be revoked, with or without cause, at the College's discretion. Web pages found to be in non-compliance may be removed immediately by the web administrator or upon failure to revise web pages and conform to these guidelines.

Accessing Data in the Administrative Systems of Emory & Henry College

The College recognizes that personnel must have access to student records and other data that is protected under the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) in order to conduct the legitimate business of the College. All Emory & Henry College administrative system users agree that use of systems maintained by partners, consortia arrangements, etc. is governed by the rules and regulations set forth in this policy. Acceptance of this policy implies cooperation with the spirit and intent of any complementing acceptable use policies which may be provided by E&H's service providers. College personnel must adhere to the following policies:

- Computers logged into Datatel, Raiser's Edge, or other administrative system applications, must never be left unattended. All users should log out of these systems whenever it is not in active use.
- No faculty or staff, office or department, should share administrative system accounts.
- Student work access to administrative systems must be strictly supervised and must be conducted only through the use of an authorized student assistant administrative system access account.

- Administrative users should not store any confidential data on hard drive, flash memory sticks, or other portable storage media. All confidential data derived from administrative systems must be stored and shared via secure password-protected folders on the network or other I.T. approved data storage locations.
- Confidential data in reports, spreadsheets, or other formats must not be emailed to other personnel. It should be stored and retrieved from password-protected folders on the network or other I.T. approved data storage locations.
- Personnel working from remote locations or taking work off campus on laptops or other portable devices must not download any data which falls under the protection of FERPA or HIPAA regulations.
- Students, faculty, employees, and others authorized by consortia partners on shared systems may be provided an account on the partner's information networks. Account privileges may include, but are not limited to, secured network storage, networked applications, databases, and Web services.
- All permanent employees who need to access the administrative systems of consortia partners will receive user account information from the consortia partner's network administrators through the Emory & Henry IT department, which is the liaison between the College and the consortia partner. Access will be revoked immediately upon termination or at the end of the last day of employment.
- Users shall under no circumstances represent themselves as others for the purpose of circumventing established policies or security measures, or for any reason without explicit permission of the others. Sharing accounts and/or passwords is a violation of this policy.

Enforcement

The Information Services Department reserves the right to enforce this policy as deemed necessary to protect the security of the network, data and files, as well as the rights and privileges of its users. These policies have been developed in consultation with IT directors from the Council of the Independent Colleges of Virginia member institutions and represent widespread practices in public and private institutions of higher education throughout the United States.

Emory & Henry College considers any violation of appropriate use principles or guidelines to be a serious offense and reserves the right to copy, examine, and remove any files or information resident on College systems allegedly related to unacceptable use and behavior. Violation of these rules will be reported to the appropriate campus office for further action. Punishments may include temporary or permanent suspension of user privileges on the network and/or disconnection from the campus network, or other sanctions as described in the Faculty and Faculty Status handbooks, the Staff handbook, or the Student handbook. Offenders may be prosecuted under laws including (but not limited to) the Privacy Protection Act of 1980, the Computer Fraud and Abuse Act of 1986, the Computer Virus Eradication Act of 1989, the Interstate Transportation of Stolen Property statutes, the Virginia Computer Crimes Act, the Electronic Communications Privacy Act, and the Telecommunications Act of 1996.

Cooperation with Law Enforcement Investigations

The proper procedures for staff members in the Emory & Henry Information Services Department regarding cooperation with and participation in investigations of suspected misconduct involving the use of the campus network or technology hardware and/ or software are as follows:

- When seeking technical support assistance from Information Services staff, each student must sign a waiver which states that the department may look at the student's personal computer files in the course of completing the requested technical support. The waiver authorizes the department to view the content of the computer's hard drive(s) in the course of completing any requested technical support assistance, if necessary in assisting the computer user.
- Should a department staff member discover potentially illegal activities, data, or files on a computer, they are to immediately document what they saw, why they came into contact with that data or file, and how they arrived there in terms of the directory structure. The staff member should take no direct action, but should notify the Director of Information Technology or Chief Information Officer immediately. If the Director of Information Technology or Chief Information Officer are unavailable, then they should notify the VP for Student Life without delay if a student is involved, or the VP for Human Resources if an employee is involved. If none of these

administrators are available, or if there is a genuine threat to public safety inferred in the discovered materials (e.g. bomb threats, plans for violent activities, etc.), then the staff member is authorized to notify Campus Security, or law enforcement officials directly if Campus Security is not available.

- Staff members are not to confiscate any personal computers or other technology that is not College-owned property.
- Staff members are authorized to remove College owned technology and return it to the Information Technology department for removal of materials which violate the Security and Acceptable Use Policy with the approval of the Chief Information Officer/Director of the Information Technology.
- Staff members are authorized to boot up computers, open files, or examine directories or folders on College-owned and non-College-owned equipment for College officials, if requested, in the investigation of suspected infractions of the Security and Acceptable Use policy if the equipment in question has been connected to the Campus network.
- Department staff members are not to release any information, data, or files, of any kind to law enforcement authorities without receipt of a properly-executed subpoena compelling the College to cooperate in a criminal investigation. Any questions or comments can be directed to the Chief Information Officer/Director of the Information Technology.