Acceptable Use Policy

Preface

Scope and Purpose

This policy applies to all users. Users are any and all individuals who access, use, maintain, program, configure, install, uninstall, or control Colgate's Electronic Information Resource (EIR). Those individuals covered include, but are not limited to all staff, faculty, students, those working on behalf of the university, guests, tenants, visitors, and individuals authorized by affiliated institutions and organizations. A user may also be defined as any person(s) who uses any Colgate University EIR regardless of whether authorized – knowingly or unknowingly. Colgate University's EIR includes electronic information, data, communication services, networks, and systems.

No student or employee of Colgate University is authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing resources owned by Colgate University.

Colgate University requires that all individuals accessing any university-provided Electronic Information Resource abide by the standards of acceptable use as indicated within this policy and its sub-policies.

Colgate reserves the right to modify or amend this policy and to limit or restrict the use of its EIR at its sole discretion. Further policy information can be found in staff, **faculty**, and **student handbooks**.

Policy

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the categories of acceptable and unacceptable use.

Passwords

1. All users will be provided with user accounts which must be password protected at all times. Password policies including the strength of the password and the time of use of the password

must be implemented and followed. See Colgate's strong password policy.

2. The account provided will grant the user access to network and other EIR resources. The account holder is responsible for the content of the data protected under his or her user account and for all activity logged on the network and university EIR under that username.
3. Users shall not share their passwords with any other person, regardless of whether such other person is an authorized user for any reason including but not limited to Information Technology Services (ITS) support, faculty, staff, administration, friends, clubs, file sharing, or other.
4. Users shall not ask for or obtain account passwords for accounts not their own for any reason. Unauthorized attempts to read another person's protected files or gain access to computers or other resources not their own are prohibited.
5. Local system administrators outside of ITS shall not override protections unless approved by ITS.
6. ITS reserves the right to utilize password-reset tools in the event of lockouts, emergencies, or investigations. Administrators and providers of university EIR and data have the additional responsibility of ensuring the integrity, confidentiality, and availability of the resources they are managing. Persons in these positions are granted significant trust to use their privileges appropriately for their intended purpose and only when required to maintain the system. Any private information obtained in carrying out these duties must be treated in the strictest confidence.
7. Circumventing user authentication or security of any host, network, or account is forbidden, unless part of job duties.

Network Usage

1. For security and network maintenance purposes, authorized individuals within Colgate University may monitor equipment, systems, and network traffic at any time to ensure compliance with the Acceptable Use Policy.
2. Effecting security breaches or disruptions of network communication is forbidden. Security breaches include, but are not limited to, accessing data of which the student or employee is not an intended recipient or logging into a server or account that the student or employee is not expressly authorized to access. "Disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
3. Port scanning or security scanning is prohibited without prior ITS approval.
4. Executing any form of network monitoring which will intercept data not intended for the student or employee is forbidden.
5. Copying or transmitting excessive amounts of data is forbidden. ITS reserves the right to disable any node on the network causing the disruption and to investigate the cause.
6. It is forbidden to connect any device that adversely affects the performance of the university networks. These devices will be taken off the network, with or without notification.

Virus Protection and Network Security

1. All devices connected to the Colgate University Internet/Intranet/Extranet, if capable, shall be continually executing university-recommended virus-scanning software with a current virus database unless overridden by departmental or group policy.
2. Introduction of malicious programs into the network (e.g., viruses, worms, Trojan horses, email bombs, etc.) is forbidden.
3. Any device that is identified as initiating or transmitting an attack on other systems (e.g., having fallen victim to a virus, worm, or break-in) is prohibited and will be taken off the network immediately and may or may not be reconnected after it has been demonstrated that it is secure in the sole discretion of Colgate University.
4. Any attempt to compromise network security safeguards using devices such as sniffers, crackers, injectors, or other devices, software, or hardware is prohibited unless approved by the university for faculty-guided educational purposes, or as used by ITS staff in accordance with their job duties.

Confidential Data

1. The university must protect all student, staff, and faculty data that is deemed private with reasonable levels of access restriction and encryption where applicable and/or regulated by federal, state, or local law. Safeguards must be in place to protect data from unauthorized disclosure. As a general rule, if the data involves any one or more of the following, only authorized personnel may have access to the information in question and all access to that data shall be audited:
2. Financial data including, but not limited to, loans, payments, salaries, wages, deductions, financial aid, balances, donations, or settlements.
3. Social Security Numbers or their foreign equivalent.
4. Personally identifiable health care information (PHI) including, but not limited to, any information involving the treatment of students, faculty, staff, or their affiliates via university health care facilities.
5. Student performance records including, but not limited to, transcripts, grades, or disciplinary actions.

Copyright

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or university protected by non-disclosure agreements or covenants, copyright, trade secret, trademark, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Colgate University. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, copyrighted movies or other audio-visual works, or other copyrighted content, and the installation of any copyrighted software for which Colgate University or the end user does not have an active license is strictly prohibited. See Colgate's copyright policy here.
2. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.

Harassment

Using Colgate's EIR to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws is prohibited. No university EIR may be used for a purpose that violates university policies, rules, or regulations or for an illegal or criminal purpose under local, state, and/or federal laws.

Electronic Communications

The following activities are strictly prohibited, with no exceptions:

1. Sending unsolicited e-mail messages such as "junk mail" or other advertising material to individuals and/or distribution lists who did not specifically request such material (e-mail spam).
2. Any form of harassment via e-mail, telephone, or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of e-mail header information.
4. Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.
6. Relaying of e-mail through Colgate servers.
7. Unauthorized creation or use of mass-e-mail (distribution) lists for the purpose of sending unsolicited e-mail to Colgate faculty, staff, or students.
8. Use of Colgate's EIR by an employee for advertising to solicit or proselytize others for commercial ventures, religious or political causes, or for personal gain.
9. Making fraudulent offers of products, items, or services originating from any Colgate University account.

10. Unauthorized provision of information about, or lists of, Colgate University students or employees to parties internal or external to Colgate University.

Systems

Colgate owned devices including but not limited to computers, tablets, peripherals (printers, scanners, multi-function devices, etc…) that are directly assigned to employees or are located in a lab or public area and open for use may be used for lawful purposes only.

Audit and Compliance

Enforcement

Any student or employee found to have violated this policy may be subject to disciplinary action, up to and including termination of enrollment or employment.

13 Oak Drive Hamilton, NY 13346
(315) 228-7000