Policy on Acceptable Use of Digital Resources

Purpose

Information technology resources are made available at Colby as shared resources intended to support and facilitate the teaching, research, and administrative functions of the College. Such resources include but are not limited to computer hardware, data and voice networks, classroom audio-visual equipment and data transmitted over the network or in storage. Students, faculty, staff, and authorized guests are encouraged to use these resources to their maximum benefit. Experimentation, exploration, and learning are promoted within common sense and legal constraints.

The purpose of this policy is to provide clear guidelines for responsible and respectful use of information technology resources to members of the Colby community and their guests.

Privileges and Responsibilities

For faculty, staff, students, vendors, contractors, and authorized guests, the appropriate use of College information technology resources is authorized so long as it does not impact College computer systems, networks, related equipment or otherwise interfere with College business activities and is not prohibited by this or other policies.

The College provides access to files and documents residing on College-owned equipment and systems (and/or transmitted via the College's data network) to outside vendors who have been contracted to provide services. College contracts with such vendors will be required to have firm provisions for the security of information and for the privacy of members of the College community who may use those services.

Account holders and authenticated users are expected to exercise care to help safeguard the reliability and security of information technology resources. Individuals assume personal responsibility for the use made of their college allocated computer accounts, including maintaining a secure and confidential password and ensuring the continued security and privacy of the account.

Resource Monitoring

Colby College values the privacy of individual users and will respect and uphold that privacy whenever possible. All contents in storage on College and College-contracted data and voice networks are subject to this policy. Subject to applicable law, the College reserves the right to access, copy, and inspect files and documents residing on College-owned equipment and systems or storage contracted by the College from outside vendors. This may include access without notice, where warranted. Monitoring of campus network traffic may be performed to assure acceptable performance and to identify and resolve problems. If conditions suggest that system or network security, integrity, or performance has been compromised, authorized Information Technology Services staff will investigate and protective restrictions may be applied until the condition has been rectified.

Investigations

While the College makes every attempt to keep digital resources secure, privacy is not guaranteed and users should have no general expectation of privacy while making use of Colby's digital resources. Under certain circumstances, under the specific direction of at least two Vice Presidents of the College, it may be necessary to access information preserved in Colby's digital infrastructure. These circumstances include investigating situations involving the health and safety of a member of the Colby community, allegations of misconduct, or information security incidents involving Colby's digital resources.

If the College is presented with a valid subpoena or court order requiring that information be produced or preserved, or directing that the College assure that its employees produce or preserve such information, the College will be bound by law to comply. In addition, to protect a student or community member's health and safety, Colby may disclose information without a valid subpoena or court order.

The Office of the General Counsel shall be contacted upon receipt of any request, subpoena or court order for information.

Prohibited Activities

IT resources may not be used in any manner prohibited by state and federal law or disallowed by licenses, contracts, or College policy. This section, while not all-inclusive, lists examples of misuse that may constitute a violation of College policy.

- Use of information technology resources without proper authorization or for the purpose of personal gain, including personal financial gain;
- Attempting to gain unauthorized access to any computer or network by hacking or malicious software;
- Access or attempts to access data or network communications other than one's own without appropriate permission;
- Use of personal network equipment, broadcast points (such as wireless access points or ad-hoc computer-to-computer networks), access points or any device found to be interfering with official Colby wireless networks. Colby ITS reserves the right to disconnect service or otherwise terminate any unauthorized device without notice;
- Sharing a password or account with any other individual or third party, with the specific exception of staff or faculty members allowing authorized support personnel to access their accounts in order to provide services appropriate to their job functions;
- Using another person's computer account, user ID or data without appropriate permission (e.g., using an account found "logged in" on a lab machine);
- Theft, including the illegal duplication of copyrighted material, or the propagation, use, or possession of illegally copied software or data;
- Damaging or tampering with files, data or voice networks, software, or equipment, including any deliberate effort to degrade, halt or otherwise compromise a system, software, data or peripheral device;
- Sending threatening messages or other material constituting harassment or other sanctionable behavior as defined in Colby handbooks;
- Using College information technology resources, including networks, as a staging ground to hack (break into) any other system without permission.

Policy Violations

Violations of this Acceptable Use Policy will be handled through standard disciplinary processes as outlined in the Student Handbook and applicable faculty and staff handbooks. Information Technology Services reserves the right to take immediate action to protect information security, system integrity, and operational continuity. Reviews of actions taken by ITS and subsequent disciplinary decisions are made by the appropriate disciplinary authority in consultation with the Chief Information Officer (e.g., the College Provost for faculty violations, the Vice President for Administration and Chief Financial Officer for staff violations, and the Dean of Students for student violations).

Approval, Review and Revisions
October 2019