Bates Acceptable Use Policy

Purpose

Information Technology resources (IT resources) are provided to members of the Bates College faculty, staff, and student body and to authorized guests to support the teaching, scholarship, research, and administrative functions of the college (for this policy, the term “Users” encompasses all of the foregoing). Such resources include, but are not limited to, data, college-owned data, computer hardware, data networks, information systems, and classroom audio-visual equipment and are available to authorized users. Users of Bates College IT resources are expected to conduct themselves in a manner consistent with the college’s Statement of Community Principles, this Acceptable Use Policy, all other College policies, and state and federal law.

This policy's purpose is to provide community members with guidelines for the responsible and respectful use of these IT resources.

Responsibilities

Users are expected to exercise care to help safeguard the reliability and security of IT resources. Users assume personal responsibility for using their college-allocated computer accounts. This responsibility begins with selecting a unique and secure password and involves maintaining that password's confidentiality to ensure the account's continued security and privacy. Users are not to use their Bates password for non-Bates accounts, share passwords with other users, or utilize the password for any other account, and no one has the right to ask for them.

All Bates-issued computing devices and accounts, e.g., Bates email, are provided for the purpose of conducting College business, and the storing of personal data on these devices or accounts is prohibited. Employees of the College should not expect access to their Bates-issued computing devices, email, voicemail, or other systems past the date of separation from the College.

Users are responsible for handling College data in accordance with Bates College’s Data Classification Guidelines and Data Usage Policy. Access to and use of data must be limited to legitimate College purposes and consistent with the data’s classification level.

IT Resource Monitoring – No Expectation of Privacy

All materials, data, communications, and information, including but not limited to email (both outgoing and incoming), telephone conversations and voice mail recordings, instant messages, and internet and social media postings and activities created on, transmitted to, received, or printed from, or stored or recorded on IT resources (“content”) for or on behalf of the College are the property of the College. Users are expressly advised to prevent misuse. The College reserves the right to monitor, intercept and review and delete, without further notice, all content on IT resources. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of messages, communications, postings, log-ins, recordings, and other uses of IT resources such as, keystroke capturing and other network monitoring technologies. Therefore, you should have no expectation of privacy whatsoever in any content on the IT resources.

Access must be given to the college in instances when a user has added personal security protection (encryption, password, or pin) to hardware, files, folders, or to college data in any format or location. The college does not monitor the contents of files as a matter of course. Still, non-intrusive monitoring of campus network traffic occurs routinely to assure acceptable performance and to identify and resolve problems. Under these circumstances, College ILS staff will hold this information and knowledge in the strictest confidence.

Acceptable Uses

All users may…

- Use IT resources to support the college's educational, scholarship, research, and administrative functions.
- Use IT resources for reasonable personal computing if it does not entail a high cost to the college, impede network operations, or violate this or other College policies.

Unacceptable Uses

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

- Attempting to gain access to any IT resource to which you do not have proper the authorization;
- Intentionally distribute viruses, malware, malicious software, hoaxes, or other items of a destructive or deceptive nature;
- Sharing your passwords with the specific exception of shared accounts in which the password is common among a small number of individuals;
- Entering, uploading, transmitting, or processing Restricted data using artificial intelligence (AI) tools, large language models (LLMs), or other automated data analysis systems that are not explicitly approved by the College for such use, including third-party or publicly available AI services
- Using another person’s computer account, user ID, or data without appropriate permission (e.g., using an account found “logged in” on a public lab machine or classroom computer);
- Theft, including the illegal duplication, downloading, or sharing of copyrighted material or the propagation, use, or possession of illegally copied software or data;
- Sending threatening messages or other material intended to harass, defame, intimidate or threaten. To be clear, the College’s policies against sexual and other types of harassment fully apply to the use of the College’s information system;
- Tampering with, willful destruction of, or the damaging of files, data networks, software, or equipment;
- Use of any IT resource as a staging ground to hack (break into) any other system;
- Use of College email account to create or sign in to any third-party service that the College has not provisioned unless these services are being used exclusively on behalf of the College.

- Unauthorized exchange or transmission of Restricted data, as defined by the College's Data Classification Guidelines, including Social Security numbers, banking or financial data, or bulk student records or reports containing information about multiple students, except where limited student specific information is exchanged for legitimate academic or administrative purposes and in accordance with College policy, through email or other electronic means.
- Using a personal email account to conduct any business on behalf of the College or sending or forwarding College-related business information to personal email accounts;
- Storing on College devices and information systems any trade secrets or confidential information that users may have acquired from their former employer or any other person or entity to whom they owe a duty to keep such information in confidence unless such storage is explicitly authorized by the College and/or third party and in accordance with applicable law.

Investigations

The college and its contractors maintain certain system and data backups and logs of email and network traffic. If the college is made aware of violations of the law and is presented with a valid subpoena or court order requiring that such information be produced or preserved or directing that the college assure that its employees produce or preserve such information, the college may be bound by law to comply.

Similarly, the college may be obligated to disclose the identity of an account holder or the identity of the person who owns a computer or other registered network device, is responsible for a college-owned device, or holds a college-assigned account used in some network transaction.

Policy Violations

Any use of College devices and information systems is subject to this policy even if such use occurs during non-work hours or off College property. All users are required to comply with this important policy. If violations are discovered or suspected, College personnel may report the activity to appropriate College officials or external authorities, where violations will be handled through standard disciplinary processes as outlined in the student handbook and the applicable staff and faculty handbooks. Information and Library Services staff may take immediate action to protect the information security, privacy, system integrity, and operational continuity. Violations involving data security, privacy, or misuse of information systems may also result in reporting obligations under applicable law or College policy.