SMITH COLLEGE 150 YEARS

‹ student affairs

Smith College Technology Policies

In This Section

Acceptable Use of Computer Resources

Approved: VP for Information Technology

Date Established: *6/30/2014*

Responsible Office: Information Technology Services

Date Last Revised: *05/13/2022*

Responsible Executive: Information Security Director, VP for Information Technology

Statement

Smith College requires that any person who uses its information technology resources and services must do so in a lawful, responsible and ethical manner, abiding by all applicable laws, regulations and college policies and codes of conduct.

provided by the institution, regardless of their individual affiliation.

Policy

Introduction:

Smith College provides information technology resources to students, faculty, staff, guests, and other members of the college community for support of its general academic mission. These resources may only be used for lawful purposes, and in a manner consistent with college policies and codes of conduct. These resources include authenticated access to college electronic services, including: access to college-owned computers and electronic devices; local and Internet network access; network file storage; electronic mail (e-mail); phone service and voice mail; licensed software; electronic media content; library electronic resources; and other network-based services and data. The college has established standards and policies for the acceptable use of these resources and expects users to be familiar with and honor them.

In addition, members of the Smith College community may have access to third-party electronic resources through their affiliation with the college, including the resources of the other institutions of Five Colleges, Inc. (Amherst College, Hampshire College, Mount Holyoke College, and the University of Massachusetts Amherst). Use of these resources by members of the Smith College community is governed by this Acceptable Use Policy and also by any applicable policy or restriction of the third-party provider.

Specific Considerations for this Policy:

Actions prohibited by legal or regulatory agencies, and / or this Acceptable Use Policy or the institutional policies of Smith College include but are not limited to:

Legal and Regulatory Acceptable Use Restrictions:

promote, canvass for, or support a political party or political candidate that in any way appears to act in violation of the college's legal requirement to remain politically neutral.

- Copying media, software, documents, or other intellectual property in violation of contractual agreement, or state or federal laws.
- Downloading, or making available for download to others, any copyright protected material such as music, shows, movies, and books, without the permission of the copyright owner.
- Use of audio, images, videos, movies, or likenesses of people without their written consent.
- Use of licensed library resources in any way other than for noncommercial, educational, scholarly or research use.

Institutional Acceptable Use Restrictions:

- Use of computer resources for the purpose of **commercial or profit-making activities** not relevant to the mission of the college.
- Use of computer resources for **fundraising, business solicitation or advertising** by groups or individuals other than officially recognized campus organizations.
- Use of **the college's name and logos** in ways that suggest or imply the endorsement of other organizations, their products, or services without appropriate approval.
- Capturing or storing **protected information** such as credit card and social security numbers on college servers or systems, except as explicitly provided by other applicable policy or procedure, without prior consent of Information Technology Services.
- Use of information technology to circumvent the intent of other campus policies.

Account Use and Information Access Restrictions:

  - For the avoidance of doubt, unauthorized disclosure includes forwarding emails or other documents with personal information or institutional classified information from college email accounts to personal email accounts.

- Disclosure of non-public student information to any person not authorized to access such information is considered a particularly serious offense. Unauthorized access, or attempting to gain unauthorized access, to other users' accounts, private files, e-mail, or other personal electronic resources.
- Unauthorized access, or attempting to gain unauthorized access, to institutional data, servers, or systems, or external services provided for institutional use.

Electronic Communications Restrictions:

- Any behavior that constitutes harassment of another individual or group.
- Use of images or text that are abusive, profane, or obscene in e-mail or on web pages.
- Unauthorized use or forging of email header information, or other deliberate attempts to misrepresent user identity.

Network Use Restrictions:

- Use of computer resources in such a manner that might cause congestion of the network, or that incapacitates, compromises, or damages college resources or services.
- Capturing or "sniffing" Smith network traffic content, or probing or scanning the network or connected devices, without prior consent of Information Technology Services.
- Implementation of network services or devices, such as DHCP services, wireless access points, or network hubs or switches, that may conflict with authorized college services, without prior consent of Information Technology Services.

privacy, the college reserves the right to examine material stored on or transmitted through any and all of its resources, such as computer disk drives, network drives, e-mail, voicemail, portable devices, other electronic storage media, internet service (including wireless networks), cloud computing, and institutionally contracted information technology services, if there is cause to believe that the standards for acceptable and ethical use are being or have been violated, if there is a threat to an individuals' safety, or when it has a legitimate work or school administration-related need to do so; and to preserve the contents in response to litigation hold requests, potential legal claims, subpoenas, or other investigations. The College also reserves the right to disclose the contents to law enforcement officials.

The Vice President for Information Technology or their delegate with appropriate consultation must review and approve in advance any request for access to the contents of electronic files, data, or folders on institutional information technology resources without the consent of the user.

Students, faculty and staff who use their personal computer, portable electronic device, portable memory media, or other electronic devices for college-related business may be required to provide access to intact business-related information and possibly the devices themselves when the college has a legally-required reason.

The college reserves the right to access the contents of students' electronic files during the course of an investigation and to disclose the contents during student conduct proceedings.

Policy Violations

Violations of this policy and related college policies should be brought to the attention of policy’s Responsible Executive, and are adjudicated according to procedures outlined in the Student Handbook and the Staff Handbook, with

Definitions

These definitions apply to terms as they are used in this policy.

- **Classified information:**
  - For this policy, "classified information" refers to any institutional information that has been classified by the information owner as requiring some level of access protection or privacy protection.
- **Protected Information:**
  - For this policy, “protected information” refers to information that is explicitly protected by state or federal law, and specifically MA GL 93H / MA 201 CMR 17.
- **DHCP:**
  - "Dynamic Host Configuration Protocol" – standard service that issues a network address to a device when it attaches to the local network.

Procedures

Procedures for compliance:

Departments must ensure that internal procedures support compliance with this policy. Review and approval of internal procedures by the policy administrator is recommended.

Related Information

Related Policies

- **ITS Policies:**
  General collection of ITS policies and procedures
- **Account Password & Security Policy:**
  Smith's central user ID account security

Additional Resources

- **Smith College Code of Conduct:** Guidance for professional conduct for all faculty, staff and students
- **Staff Handbook:** General information all staff members should know
- **Student Handbook:** General information all students should know

In This Section

Electronic Mail Policy ›

Policy on Use of Email for Official College Communication ›

Wireless Network Policy ›

Smith College

10 Elm Street
Northampton, MA 01063

Phone: 413-584-2700