COMPUTER POLICIES

Sweet Briar College | 134 Chapel Rd Sweet Briar Virginia 24595

Tables of Contents

I. Academic Freedom

A. General

Principle
The principles of academic freedom apply to academic computer systems. Computer polices of Sweet Briar College are consistent with general university codes and widely accepted statements on academic freedom such as the Joint Statement on Rights and Freedoms of Students. (Appendix A)

B. Policy Formulation
Sweet Briar College has an obligation to clarify those standards of behavior which it considers essential to its educational mission and its community life. These general behavioral expectations and the resultant specific regulations represent a reasonable regulation of conduct, but the computer should be as free as possible from imposed limitations that have no direct relevance to her education or to the pursuit of the business of the college. Offenses should be as clearly defined as possible and interpreted in a manner consistent with the aforementioned principles of relevance and reasonableness. Disciplinary proceedings will be instituted only for violations of standards of conduct formulated with significant community participation and published in advance through the generally available body of institutional regulations.

C. Student and Faculty Discipline

Principle
Suspension or expulsion from a computer is a serious penalty. Users facing these penalties will be given due process protection similar to that given to those facing other serious penalties as delineated in Faculty Rulings and the Student Handbook.
Interpretation
"Pending action on the charges, the status of a user and her files/data should not be altered, or her right to be present on the campus and to attend classes [and use computers] suspended, except for reasons relating to his physical or emotional safety and well being, or for reasons relating to the safety and well-being of students, faculty, or college property." [Joint Statement]

D. Privacy

Principle
Personal files on college computers (for example, files in a user's home directory or on a personal computer connected to the college network) should have the same privacy protection as personal files in dormitory space or living space assigned by the college. Private communications via computer should have the same protections as private communications via telephone.

E. Computer Expression

Highest
All education, research, and administrative purposes of the college.

Medium
Other uses indirectly related to Sweet Briar purposes with education or research benefit, including personal communications.

Lowest

Recreation, including game-playing.

Forbidden

Selling Sweet Briar resources, commercial activities not sanctioned by the President's office, intentionally denying or interfering with service, unauthorized use or access, reading or modifying files without proper authorization, using the technology to impersonate another, violations of laws or other Sweet Briar policies.

Interpretation

"Academic institutions exist for the transmission of knowledge, the pursuit of truth, the development of students, and the general well-being of society. Free inquiry and free expression are indispensable to the attainment of these goals. As members of the academic community, students should be encouraged to develop the capacity for critical judgment and to engage in a sustained and independent search for truth." [Joint Statement]

Principle

The principles of intellectual freedom developed by libraries should be applied to the administration of information material on computers. These principles are explained in such American Library Association documents as the Library Bill of Rights, the Freedom to Read Satement, and the Intellectual Freedom Statement.

Interpretation

Computer sites that offer newsgroups should select newsgroups the way that traditional libraries select magazines and books.

Interpretation

"Every [academic computer] system should have a comprehensive policy on the selection of [information] materials." [ALA Workbook for Selection Policy Writing] However, the mission statement of Sweet Briar College is the primary guiding principle and selection may be affected by institutional policy and the availability of computing resources.

Interpretation

"Materials should not be proscribed or removed because of partisan or doctrinal disapproval" [Article 2, Library Bill of Rights].

Principle
The principles of academic freedom applicable to student and faculty publication in traditional media, apply to student and faculty publication in computer media.

Sweet Briar College provides and maintains computing and telecommunications technologies to support the education, research and work of its faculty, staff, and students. Sweet Briar's computing and telecommunications technologies are collectively referred to as SBCNet. By connecting computers with each other and with national and international computer networks, SBCNet provides many educational benefits.

The purpose of this policy is to define responsible and ethical behavior of SBCNet users in order to preserve the health, availability, and integrity of college computing resources. This policy is purposely silent on matters covered by other policies such as sexual harassment and honor code violations, and by federal and state laws on privacy and computer abuse. This policy applies to all users of Sweet Briar computing resources.
The priorities for use of Sweet Briar computing resources are:
Because it is not possible to anticipate all the ways in which individuals can harm or misuse college computing facilities, this policy focuses on a few simple rules. These rules generally indicate actions that should be avoided.
If you observe someone violating this policy, or another Sweet Briar policy using SBCNet resources, you can report it by email to stopit@sbc.edu. Many local computing systems also have a "stopit" account that you can send mail to in order to report questionable activities Ñ alternatively you may send mail to postmaster@sbc.edu.

II. Computing Use

A. Rules of Use

Sweet Briar treats access to SBCNet resources as a privilege that is granted on a presumption that every member of the college community will exercise it responsibly. The following rules are not complete -- just because an action is not explicitly proscribed does not necessarily mean that it is acceptable. The rules should be read for the principles behind them and the principles adhered to in all situations.

- Use SBCNet Consistently With the Stated Priorities.
  Low priority uses of SBCNet should be avoided during the times of peak demand, typically the midafternoon to late evening hours. During peak periods, other users may be prevented from doing their high priority work if you are doing something of low priority. Those users are likely to complain to you or to if they observe you interfering with their work.
  Certain activities such as chain letters, broadcast email, transmission of large image and sound files, to very large distributions will consume large amounts of resources; avoid them.
- Don't Allow Anyone to Use Your Account.
  Your Sweet Briar username identifies you to the entire international Internet user community. Another person using your account, whether or not you have given permission, will be acting in your name. Anyone who knows your password can use your account. You are responsible for that person's actions in your account. If that person violates any policies, his or her actions will be traced back to your username and you may be held responsible. The easiest way to protect yourself is to not give away your password. If you need to give someone access, give it on a temporary basis, and change your password immediately after that person finishes using your account. You should also not give your password to anyone you do not trust.
  If someone else offers you use of an account for which you are not authorized, decline. If you discover someone's password, don't use it; report the access to the password to the owner or to stopit@sbc.edu.
- Honor the Privacy of Other Users.
  Sweet Briar treats the contents of all files, email, and communications as private, and will strive to protect the privacy of all users. Many aspects of privacy of files and communications are also protected by Federal and State laws. Examples:
- Don't access the files or directories of another user without explicit authorization from that user. Typically, authorization is signalled by the other user's setting file access permissions to allow public or group reading of files. Since some systems by default make all files readable to all users and some users don't know this, the file permissions are not reliable. It is always best to ask.
- Don't intercept or monitor any network communications not explicitly meant for you.

- Don't use the systems or transmit personal or private information about individuals unless you have explicit authorization from the individuals affected. Don't distribute such information unless you have permission from those individuals.
- Don't create programs that secretly collect information about users. Software on SBCNet is subject to the same guidelines for protecting privacy as any other information-gathering project at the college. You may not user computer and telecommunication systems to collect information about individual users without their consent. Note that some system utilities log user information (ftp, mosaic, login, etc.). This is considered normal system administration functions.
- Don't Impersonate Any Other Person.
  Using SBCNet resources to impersonate someone else is improper. If you use someone else's account, you may be committing acts of fraud because the account owner's name will be attached to the transactions you have performed.
  If you send anonymous mail or postings, you should realize that it is customarily considered polite to identify that your message is anonymous or is signed by pseudonym. You should be aware that most people will give less credence to anonymous communication than to signed communication.
- Don't Use SBCNet To Violate Other Policies or Laws.
  Computer networks offer new ways to commit actions that violate laws or policies that are covered elsewhere. Here are reminders of typical other policies:

- Don't copy copyrighted documents. Many programs and their documentation are owned by individual users or third parties and are protected by copyright and other laws, licenses, and contractual agreements. You must abide by these restrictions; to do otherwise may be a crime. (See Appendix D: Policy on Unauthorized Copying)
- Don't use SBCNet to threaten or harass anyone. Various types of harassment, including sexual, religious and racial, are proscribed by SBC policies.
- Don't use SBCNet to violate the Honor Code.
- Don't use SBCNet to launch viruses, worms, trojan horses, or other attacks on computers here or elsewhere.

B. Offices, Centers, and Departments

Organizational units on the campus operate computers and networks to support their missions. The principles of this policy apply to all Sweet Briar organizational units, and any computers connected to SBCNet. Units may set additional local policies and expectations that are consistent with this policy.

C. Privacy

All users of SBCNet enjoy a right of privacy. No other user, system administrator, or official may read email, files, or communications without the consent of their owners. Only in rare and exceptional cases where a severe threat is present and there is no alternative to ameliorating the threat may the Director of Computing authorize the reading of email, files, or communications. No system administrator or official may do this without the authorization of the President or Dean.

D. System Administrators

The system administrators of various computers around campus have special responsibilities. They should exercise their extraordinary powers to override or alter access controls, accounts, configurations, and passwords with great care and integrity. System Administrators manage computers and administrate policies, but they do not create policies. Their actions are constrained by this policy and by

the policies of local administrative units. In particular, local units should set policies concerning accounts on their machines, and system administrators must follow these policies.
If a system administrator observes someone engaging in activities that would seriously compromise the health or integrity of a system or network — e.g., someone launching a virus attack or attempting to gain root access — she may take immediate action to stop the threat or minimize damage. This may include termination of processes, disconnection from a network, or temporary suspension of an account. Account suspensions must be reported immediately to the Director of Computing. Only in exceptional cases may personal files or communications be inspected. Thus, computing personnel may not read email, files, or communications as part of an investigation without explicit authorization.

E. Security Review Panel (SRP)

This policy establishes a Security Review Panel consisting of the Director of Computing, the Networks Manager, a student to be selected by the Network Services Division, a faculty member selected by the Technology Planning Group, the Director of Libraries & Integrated Learning Resources, Computer Resources/Technical Support Coordinator, and the Dean of the College or her/his designee. Its chair will be the Director of Libraries and Integrated Learning Resources. Computing administrators will report all violations and their responses to this panel immediately. Any member of the community can report a violation to the panel via stopit@sbc.edu. On receipt of a complaint from a community member, the panel chair will assign one of the members as the panel's "case worker" for that complaint. The five-step "stopit process" within which the panel operates is described below. If a user's account is disabled as a result of a suspected violation, the user has a right to a resolution and reactivation of the account in the case of a mistake within 2 working days. The panel is also responsible for reviewing these policies periodically and recommending improvements and clarifications as needed.

F. Responsible Use of Computing

The Stopit Process

Sweet Briar's computing policy document provides rules of use for the campus computing and telecommunications technologies. This document, which complements those policies, defines the process for handling policy violations.
The process described here, called "stopit" after a similar process at MIT and George Mason University, uses a graduated approach to deal with violations of the policy. The approach is based on the premises that the vast majority of the users are responsible and that most offenders, given the opportunity to stop uncivil or disruptive behavior without having to admit guilt, will do so and will not repeat the offense. Many offenses are not direct threats to the integrity of Network Sweet Briar itself, but are violations of other campus rules, state laws, or federal laws for which there are enforcement processes already in place. The stopit process is designed to direct complaints to the appropriate authorities quickly. The stopit process has five stages:

STOPIT 1: Wide Distribution of Policy Information
A poster describing the essence of the responsible use policy will be displayed in each computer lab on the campus; the same information will be given to new users and to each user annually. The essence of the policy is that certain behaviors may interrupt or hurt other members of the SBC community; all users should refrain from such behaviors. Anyone observing a harmful or disruptive behavior can report it to stopit@sbc.edu or to the campus police.

STOPIT 2: Standard for Registering Complaints

The stopit@sbc.edu address is monitored regularly by members of the Security Review Panel (SRP), who will make sure that complaints are responded to rapidly. In many cases, the SRP member who responds

to a complaint will alert the existing authority who handles the type of complaint — e.g., accusations of sexual harassment go to the campus sexual harassment board, honor code violations to the honor committee, thefts of equipment to the campus police, repetitive misconduct to the Dean of Co-Curricular Life, chain-letters to the network Postmaster. Users do not need to know who the proper authority is for a particular complaint, they simply write to stopit@sbc.edu.

STOPIT 3: Warning Letter

The third mechanism, which almost always follows STOPIT 2, is a letter to the alleged perpetrators of improper Network Sweet Briar use, harassment, or other uncivil behavior. The letter will have this form: "Someone using your account did [whatever the offense is]." This is followed by an explanation of why this behavior violates which policy. "Account holders are responsible for the use of their accounts. If you were unaware that your account was being used in this way, it may have been compromised. The system administrator of the machine hosting your account can help you change your password and re-secure your account. If you were aware that your account was being used to [do whatever it was], then please make sure that this does not happen again." Finally, the letter will identify an SRP member who has been assigned to the case.
This stage makes sure the persons are informed of the policy violation and complaint and offers them the chance to desist without having to admit guilt.

STOPIT 4: Mandatory Interview with SRP Member

If the recipient of a STOPIT 3 letter wishes to contest what is said in the letter, he or she may talk to the SRP member assigned to the case. If that recipient repeats the offense, or commits a new offense, he or she will be invited to a mandatory interview with the SRP member assigned to the case. The SRP chair can authorize the temporary suspension of access to an account if the individual fails to arrange for the mandatory interview. Individuals may request a hearing before the full SRP.

STOPIT 5: Disciplinary Procedures
If none of the previous stopit stages convinces the offender to desist, the matter will be referred to the normal university disciplinary procedure for the type of offense. The SRP will make available all information and evidenceit has on the case to the disciplining authority.

III. Data Security

A. Statement of Need

Sweet Briar College relies increasingly on data stored in information processing systems on a wide variety of computing resources at the college to satisfy the college information requirements and to further its educational mission. Security of this data, its proper, lawful use and access to that data is essential. The data must be both maintained accurately and stored and transmitted securely if the institutional mission as well as college, federal and state regulations regarding privacy and freedom are to be followed. Obligations regarding institutional data apply to that data whether it is maintained on centralized administrative systems or on computers located in offices or other campus buildings. Considerations regarding privacy, security and proper disposal applying to paper copies of information apply as well to electronic data. Where data is transferred from institutionally owned computers to computers used by employees of the institution in other locations, e.g., at home or travelling, all policies regarding data security and confidentiality shall apply.

B. Lawful Use and Access

The data policies of Sweet Briar College are covered under applicable Federal laws and regulations and the laws of the Commonwealth of Virginia. College policies are consistent with all applicable regulations.

C. Data Privacy

Members of the Sweet Briar community are responsible for ensuring that their uses of the college's data are consistent with the college policy on privacy of information.

Rationale

The college commitment to protect the personal privacy of members of the Sweet Briar community is long standing and strong. It is clearly expressed in policy, in elements of the organization's structure, and in practice. “Recognizing that specific items of information about individual students, faculty, and staff (as well as former students, faculty and staff) must be maintained for the educational, research, and other institutional purposes of Sweet Briar, it is college policy that such information be collected, maintained, and used by the college only for appropriate, necessary, and clearly defined purposes, and that such information be controlled and safeguarded in order to insure the protection of personal privacy. ..Such information should not be used or exchanged within the college for purposes other than those stated or related, legitimate purposes that would be reasonably expected."

Implications

The Institute's policy on privacy of information applies for all the colleges data, regardless of the storage form or location. With the rapid proliferation of information technology in college offices and the interest in new applications, such as computerized phone directories, protection of individual privacy will occur only if all members of the community know about the policy and are diligent about complying with it.
Recipients of confidential data in files downloaded to workstations must maintain the confidentiality of those data. People who develop new applications in central offices or other departments must assure that their use of information conforms with the privacy policy. They will, for example, have to notify students and staff when information about them, collected for other purposes, will be put to a new use and give people the chance to refuse to have data about themselves included.

Implementation

Contents of the various policy and procedure communications on this subject will be coordinated to assure that all members of the community understand the policy on Privacy of Information and their responsibilities for compliance with it, for both computerized and manual records in all offices.

D. Data Custodian

It is the responsibility of the designated custodian of a particular data collection to ensure data integrity, security and accessibility to all who demonstrate need.

Rationale

Among all the business data stored in many locations at the college, certain collections of data have been designated the official records of Sweet Briar College, and certain officers of the college have been designated the custodians of those official records.

The practice of custody has over the years been extended to include implicit custodianship of the computerized data from which official records are now usually printed. Although it is appropriate that ownership of the data be assigned to the college and accessibility be available to all who demonstrate need, it is also necessary to designate an identifiable focal point for assuring the protection of the records' accuracy, integrity and security.

Implications

The roles and responsibilities of custodians for computerized information must be clear and broadly understood. The responsibilities are complex, balancing the sometimes competing demands of daily operations, accessibility, privacy, legal constraints, and accuracy. Efforts to resolve complexities can lead individual custodians to differing interpretations of their roles. The differences may have frustrating results, especially for those who need to combine information from more than one data collection, as many departmental administrators do.
Identification of custodians must be explicit, but is increasingly complicated as offices share information and computerized databases. Resolving custody identification issues may impact current organizational forms.

Implementation

A custodian will be identified for each collection of administrative data. For those data collections that cross organizational boundaries, the custodianship of individual data elements will be established. Responsibilities of custodians for the data's logical and physical integrity and for responding to requests for access to the data will be clarified and communicated to all concerned.
Custodians will provide information about the data collections to the Director of Computing for the directory of the collections of the college's information.

E. Statement Regarding Ownership of Information

Where information regarding the business of Sweet Briar is provided for use outside the college, it shall be transmitted with the following statement appended:
"This information is the property of Sweet Briar College and herein reserved as proprietary information. No part of this information may be disclosed or used without proper written consent of an authorized representative of Sweet Briar College."
Data provided for purposes of public relations and information, for the dissemination of scholarly activity, and that designated as directory information shall be governed by appropriate college policies, federal and state regulations and accepted practices of scholarly communication.

F**. Action Regarding Violation of Policy**

Violations of data security policies as well as guidelines, standards and procedures pursuant to these policies may be grounds for disciplinary action. Such action is in addition to any criminal or civil liability under applicable laws that may result from violations.