

XIV. INFORMATION TECHNOLOGY POLICY (Faculty Meeting, May 19, 2000)

A. Account Policy

1. The computer and networking resources are the property of Whitman College. Every student, faculty, and staff is entitled to an account to access those resources. The account is for the exclusive use of the user who is assigned the account and password. Lending of an account to another person is not permitted, and is considered to be a violation of College policy and may result in disciplinary action. The College does not sell, share or rent account information in ways different than are described in this policy.

2. The Whitman College "Privacy Policy" describes the user's right to privacy.

a. Limitation

The Whitman College "Acceptable Use Policy" describes limitations on the usage of accounts.

b. Suspension of Accounts

The Whitman College "Acceptable Use Policy" describes those actions that may lead to suspension of accounts.

c. Upon Leaving the College

1) Graduating students have access to their accounts for one year after graduation. Extensions beyond the one-year period will not customarily be granted. After one year, students have an option to participate in the life-long e-mail forwarding service through the Office of Alumni Relations.

2) Students who leave the institution without graduating (e.g., transfer, dismissal, etc.) will have access to their accounts for one month following the termination of their relationship with the College. Students on leave of absence (including study abroad) will have their accounts retained.

3) Faculty or staff who permanently retire may keep their account for life.

- 4) Faculty who leave the College for other reasons will have access to their accounts for six months following the termination of their relationship with the College. If a longer period is desired, contact the Chief Technology Officer.
- 5) Staff who leave the College for other reasons will be evaluated on an individual basis. Generally, staff accounts will terminate immediately.

B. Privacy Policy

1. This policy addresses the College's commitment to protecting the privacy of authorized users of its Information Technology (IT) systems, and other systems that are capable of recording information about the user. Hereinafter these authorized users are referred to as "The Whitman Community". Despite the College's adherence to these policies it cannot assure the Whitman Community protection from the sorts of activities broadly referred to as "hacking" whose consequence might be a loss of electronic privacy.
2. The Chief Technology Officer reminds the Whitman Community of the inherent insecurity of electronic information particularly on the Internet, and of their responsibility in ensuring the privacy of their account (e.g. users should use a secure password, not share their passwords or access to their accounts, etc.).
 - a. The College is committed to protecting the privacy of the Whitman Community as it concerns materials stored on College computers or transmitted electronically on College networks or Information Technology (IT) infrastructure. In the event of court cases, it will make every reasonable effort to defend users' privacy. Whitman College will not access or monitor computer accounts, usage of IT services, or other electronic records except when:
 - 1) authorized by the user(s)
 - 2) performing maintenance necessary for the operation of the relevant systems, in which case the user(s) shall be notified of such access
 - 3) necessary for billing purposes (e.g. long distance) or legally required to do so, after the College has

mounted a reasonable effort to defend the privacy of the user(s).

- b. Routine maintenance and upkeep that do not involve examination of account or network traffic content or information content in general, such as backups, are exempt from the notification requirement.
3. While it is necessary to store some information about users and individual use of electronic services, neither this information nor knowledge derived from this information will be accessed unless:
- a. it is fundamentally necessary for the functioning of the College's IT or electronic infrastructure or
 - b. there is clear evidence suggesting that the security and/or the integrity of the system is being compromised.

In either of these cases only the Chief Technology Officer or his/her designees will make use of this information or its derivatives and then only in their efforts to assure the smooth functioning of the College's IT resource and other electronic systems.

4. Whitman College is committed to the free flow of ideas, and the freedom of electronic speech shall be fully protected. The College will actively protect the Whitman Community's freedom of expression. The content of electronic communication is not censored; this includes, but is not limited to, personal web pages, postings to listservs and newsgroups, and e-mail. However, in accordance with the principles of this policy, the following limitations apply:
- a. the volume of information may be limited without regard to content because of the technical constraints of the system (e.g., the number of news groups available at any one time may be limited).
 - b. The College retains the right to protect itself from liabilities posed by the electronic behavior of members of the College, if these behaviors are patently illegal. Otherwise the College will make every reasonable effort to defend users whose rights for freedom of expression are being challenged.

- c. Users are expected to abide by the laws of the State of Washington and the United States and by the policies of the College.

C. Acceptable Use Policy

1. Introduction

The Whitman Campus Network is provided as a service to students, faculty, staff, and other members of the Whitman community. Maintained by Whitman College Technology Services (WCTS), the Network supports the instruction, research, and service mission of the College. This document outlines the policy of acceptable use of Whitman Campus Network resources, the effective protection of individual users, equitable access, and proper management of those resources.

2. Individual Responsibilities

- a. Whitman College strives to provide fair and distributed access to computing and network facilities for the entire community of users. It is the intent of Whitman College to make available unfiltered information on the Internet for the College community. Members are responsible for selecting, viewing, and utilizing resources. If it is necessary to filter or block any information to enhance security or performance, and if this filtering or blocking occurs regularly or more often than occasionally, a description of and rationale for the action will be posted with other WCTS online information.
- b. To foster trust and intellectual freedom, it is necessary to practice courtesy, common sense, and restraint in the use of shared resources. Improper use of Whitman facilities may prevent others from gaining fair access to those facilities.
- c. Furthermore, users must keep in mind that networks or systems outside of Whitman College (including those in other countries) may have their own distinctive policies and procedures. Users are advised to learn and abide by the policies and procedures of these external networks.
- d. Insofar as a secure and reliable computer system is necessary to the academic mission of the College, all members of the College community should contribute to

the security of the system by conscientiously protecting their access privileges, for example: users need to select a secure password and, furthermore, should change their passwords frequently. Likewise, the computer system administrators will act promptly when evidence of serious compromises to the security of the system is detected.

e. The Whitman College computing network must work within finite limitations of bandwidth and disk space. Users are reminded that electronic mail exists on a space shared by other members of the community, and users are responsible for maintenance of their electronic mailbox. Therefore users are encouraged to keep only pertinent materials in their mailbox accounts. The user should:

- 1) conserve disk space: delete unwanted e-mail messages as soon as possible and arrange for forwarding of e-mail when appropriate (e.g. breaks, overseas study).
- 2) be aware that e-mail cannot be guaranteed to be perfectly private: others may intentionally or unintentionally forward or print your message, making it publicly available.
- 3) Like electronic mail the maintenance of a user's own storage area is the user's responsibility. The user should:
 - a) conserve server disk space
 - b) routinely and frequently check for viruses.
 - c) not maintain anything that the user considers to be private in the network storage area. (Files in network storage may be accessible by persons with system privileges.)

3. Conduct

Activities that violate the Acceptable Use Policy include, but are not limited to, those in the following list:

- a. Using a computer account that does not rightfully belong to you.

- b. Violating copyright laws and their fair use provisions through inappropriate reproduction or distribution of copyrighted files (including movies, music, computer software, text, and images).
- c. Using the Campus Information Technology (IT) infrastructure to gain unauthorized access to other computer systems.
- d. Unauthorized connecting of equipment to the campus network (this includes personal hubs in rooms).
- e. Attempting to break into the system by circumventing data protection schemes or uncovering security loopholes. This includes the wrongful use of programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- f. Knowingly or negligently performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- g. Attempting to damage or to place excessive load on a computer system or network by using programs, such as (but not limited to) computer viruses, Trojan Horses, and worms.
- h. Deliberately wasting or overloading computing or printing resources, or deliberately using excessive bandwidth on the network.
- i. Violating terms of software licensing agreements.
- j. Using College resources for non-academic commercial activity such as creating products or services for sale, without express College approval.
- k. Using electronic mail or other Information Technology resources to abuse, harass, or intimidate members of the College community on any basis including race, ethnic origin, creed, gender or sexual orientation. Users are reminded that sexually suggestive materials displayed inappropriately in public places, the classroom, or the workplace may constitute sexual harassment.

- l. Propagating mass mailings with the intent of flooding ("spamming" or "bombing") the accounts of others.
 - m. Forging the identity of a user or machine in an electronic communication.
 - n. Transmitting or reproducing materials that are slanderous or defamatory, or that otherwise violate existing laws or College regulations.
 - o. Attempting to wrongfully monitor or tamper with another user's use of the College's Information Technology infrastructure (such as reading, copying, changing, or deleting another user's files or software) without the knowledge and agreement of the owner.
4. Authorization
 - a. Personal use of Whitman College computing resources by staff employees during working hours is an issue that will be determined by the employee's supervisor.
 - b. Use of College computing and network facilities for non-academic commercial monetary gain requires the approval of the College and may require a written contract that gives full details of any financial obligation and/or charge for use, if any.
 - c. Connecting network devices, such as "network hubs" to the campus system will require authorization from the Chief Technology Officer or his/her designee.
 - d. Setting up a new domain on a computer located on the Whitman College network will require authorization from the Chief Technology Officer or his/her designee.
 - e. Authorization decisions may be appealed to the appropriate Dean or supervisor.
5. Enforcement of Policies
 - a. Failure to comply with any of the above policies may result in termination of network privileges, College disciplinary action, and/or criminal prosecution.

- b. It is understood that users may unwittingly create problems for others by, for example, employing programs that monopolize the network bandwidth. In such cases the Chief Technology Officer (or his/her designate) will contact the user and explain why and how the user needs to modify his or her electronic behavior. A policy clarification letter may be written. In cases of repeated problematic behavior, the CTO may recommend to the appropriate Dean or supervisor that a formal warning be placed in the user's College record. If so, the user will be notified of this recommendation and will be allowed the opportunity to provide a response to the recommendation in advance of the Dean's/supervisor's decision.
- c. Access to computing resources may be suspended temporarily at any time by the Chief Technology Officer (or his/her designate), if there is clear evidence to suggest that the resource(s) are being used in a manner that seriously compromises the security and/or integrity of the resource(s). In such a case, the owner of the account will be sent notification of this action within twelve hours and assisted in extracting such files as are immediately needed (e.g., for class assignments) and/or establishing a new, secure account, as appropriate.
- d. Upon suspension, a user shall discuss the issue with the Chief Technology Officer (or his/her designate) in order to reestablish an account. The account shall be reestablished within one business day of a satisfactory conclusion to this meeting. If the account is not reestablished to the user's satisfaction, he or she may appeal to the appropriate office of the College. The Chief Technology Officer (or his/her designate) may also choose to refer the case for disciplinary action in accordance with established procedures. For students, it is as described in Part 5, Section 2 of the Whitman College Student Handbook. For faculty, see Faculty Handbook; for staff, see Staff Handbook.