

# Acceptable Use Policy

Section Navigation



## 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.

## Individual Responsibilities

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.

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.

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.

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.

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:

- a. conserve disk space: delete unwanted e-mail messages as soon as possible and arrange for forwarding of email when appropriate (e.g. breaks, overseas study).
- b. be aware that email cannot be guaranteed to be perfectly private: others may intentionally or unintentionally forward or print your message, making it publicly available.
- c. 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.)

## 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

- ...intentionally, 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.

## 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 Information Officer or his/her designee.
- d. Setting up a domain on a computer located on the Whitman College network will require authorization from the Chief Information Officer or his/her designee.
- e. Authorization decisions may be appealed to the appropriate Dean or supervisor.

## Enforcement of Policies

Failure to comply with any of the above policies may result in termination of network privileges, College disciplinary action, and/or criminal prosecution.

privileges, college disciplinary action, and/or criminal prosecution.

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 Information 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 CIO 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.

Access to computing resources may be suspended temporarily at any time by the Chief Information 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.

Upon suspension, a user shall discuss the issue with the Chief Information 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 Information 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.

---

Approved by the Whitman Faculty - May 19, 2000 Amendment approved by the Whitman Faculty - March 17, 2004

ADMISSION: 509-527-5170

345 Boyer Ave.

Walla Walla, WA 99362