STANDARDS OF CONDUCT

INFORMATION TECHNOLOGY

[Policies developed by Information Technology Services and reviewed by the faculty, May 1997, revised June 2002, June 2005]

Introduction

Information Technology (IT) is now integrated into almost every aspect of university life for students, faculty and staff members. In the rapidly changing area of information technology one requirement remains constant: all information technology use must fully respect the rights of the University and its community members.

Most use of IT parallels familiar activities in other media and formats and so existing University policies as represented in The Faculty Handbook already provide guidance. Using electronic media in the place of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor will it alter the guiding policies: University policies which already apply to freedom of expression, privacy and related matters apply to electronic expression as well. These Information Technology Policies address circumstances which are new or at least unfamiliar in the IT arena, but they augment rather than replace other applicable University policies.

Purpose

The purpose of University Systems is to further the research, education, and administrative functions of Wesleyan University.

To achieve this purpose, these policies intend:

- to ensure the integrity, reliability, and good performance of University Systems;
- to ensure that the community of users at Wesleyan operates according to the same conventions and values as the larger Wesleyan community;
- to ensure that University Systems are used for their intended purposes; and
- to establish sanctions and processes for addressing violations.
Definitions

University Systems include the computers, terminals, printers, networks, modem banks, phone system and related equipment, as well as data files or documents residing on disk, tape, or other media which are owned, managed or maintained by Wesleyan University. For example, University Systems include institutional, departmental and faculty research systems and general access computer facilities. Privately owned equipment is not a University System even if it is attached to the Wesleyan network unless that equipment is managed or maintained by Wesleyan University.

A User is any person, whether authorized or not, who makes any use of any University System from any location. For example, this definition includes persons who access University facilities via an electronic network or who are present in University computer clusters, as well as those who use a University electronic network to connect a personal machine to any other system or service.

A University User is a user with authorization to access a non-public University System. University Users include Wesleyan students, faculty members, staff members, and alumni or alumnae with accounts on University Systems. Levels of access and authorization will vary depending on the individual’s role in the University.

A System Administrator is an individual with the authority to determine who is permitted access to a particular system.

Scope

Wesleyan's Information Technology Policies apply to all University Systems and their use. For example, all use of Wesleyan's network is subject to these policies.

Many University Systems (Wesleyan's World Wide Web sites, File Servers, University email services, individual research lab systems, etc.) sometimes have service-specific policies which apply in addition to these institutional policies. Please refer to postings available with each system to identify all applicable policies.

The policies described herein are those that the University intends to use in normal operation of its facilities. This document does not waive any claim that Wesleyan University may have to ownership or control of any hardware,
Information Technology

software, or data created on, stored on, or transmitted through University Systems.

The use of University Systems, even when carried out on a privately owned computer that is not managed or maintained by the University, is governed by this policy. This includes access to University Systems from non-campus locations.

Use of University Systems

Proper Authorization
Use of non-public University Systems is restricted to University Users.

Appropriate Use
University Systems may be used only for their intended, authorized purposes. For example, privately owned computers may not host sites for non-Wesleyan organizations across the Wesleyan network without specific authorization.

Commercial Use
Without specific authorization, activities using University Systems for non-Wesleyan commercial purposes are prohibited. This is not meant to restrict normal communications and exchange of electronic data, consistent with the University's education and research roles, that may have an incidental financial or other benefit for an external organization. For example, it is appropriate to discuss products or services with companies doing business with Wesleyan or to contribute to on-line forums discussing issues relating to commercial products. Inappropriate use would include activities such as using a Wesleyan-based web site to run a personal for-profit business.

Contracts
All use of University Systems must be consistent with all contractual obligations of the University, including limitations defined in software and other licensing agreements.
Privileges for University Users

Limited Confidentiality
Systems Administrators will identify categories of data, such as electronic mail which will be managed as confidential on a particular University System and they will make all reasonable efforts to maintain the confidentiality of that data. However, limits and risks do apply to confidentiality, due, for example, to technical limitations, software bugs, and system failures. Systems Administrators will take reasonable steps to inform University Users of limits to confidentiality for their respective University Systems. University Users are expected to become familiar with those limits and risks of confidentiality in the University Systems which they use and to manage their confidential data accordingly.

Whenever possible and appropriate, ITS will attempt to notify users of any unusual access to their electronic data. There are, however, circumstances in which, following carefully prescribed procedures, the University may determine that certain broad concerns outweigh the value of a User’s expectation of privacy and warrant University access to relevant University Systems without the prior notification of the University User.

The following conditions are examples of adequate cause for accessing data residing in University Systems without User notification.

1. When necessary to identify or diagnose system or security vulnerabilities and problems, or otherwise preserve the integrity of the University Systems.
2. When required by federal, state or local law
3. When the University has been informed that a violation of law or University Policy may have taken place and inspection or monitoring may produce evidence related to the misconduct
4. When required to preserve public health or safety

Fair Process
University Users have the right to fair process in cases of discipline resulting from policy violations. See Enforcement Procedures, below.
Responsibilities for All Users

Personal Account Responsibility
Users are responsible for the security of their University System accounts and passwords. Any user changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single users and are not to be shared with any other person without authorization by the cognizant Systems Administrator.

Users are presumed to be responsible for any activity carried out under their University System accounts.

Unauthorized Use
Users must not permit or assist any unauthorized person to access University Systems. Non-public University Systems may not be used by any non-Wesleyan organization, for example, without appropriate authorization.

Security
Users must not defeat or attempt to defeat any University System's security, for example, by 'cracking' or guessing user identifications or passwords.

Unauthorized Data Access
Users must not access or attempt to access data on a University System they are not authorized to access. Users must not make or attempt to make any deliberate, unauthorized changes to data on a University System. Users must not intercept or attempt to intercept data communications not intended for that user's access, for example, by 'promiscuous' bus monitoring or wiretapping.

Concealed Identity
Users must not conceal their identity when using University Systems, except when anonymous access is explicitly provided. For example, users must not masquerade as or impersonate others.

Denial of Service
Users must not deny or interfere with or attempt to deny or interfere with service to other users by means of "resource hogging," distribution of computer worms or viruses, etc. Knowing or reckless distribution of unwanted mail or other messages is prohibited.

Uses of computer resources that may cause excessive network traffic or computing load are prohibited. For example, a User sending out thousands of emails which included a large attachment would seriously compromise the performance of the email system.
Copyright
Users must observe intellectual property rights including, in particular, copyright laws as they apply to software and electronic forms of information.

For example, running a program which allows illegal sharing of copyrighted music or video is prohibited.

External Data Networks
Users must observe all applicable policies of external data networks when using such networks.

Modification of Data or Equipment
Without specific authorization, users of University Systems must not cause, permit, or attempt any destruction or modification of data or computing or communications equipment, including but not limited to alteration of data, reconfiguration of control switches or parameters, or changes in firmware. This rule protects data, computing, and communications equipment owned by Wesleyan University, or any other person or entity. 'Specific authorization' refers to permission by the owner or Systems Administrator of the equipment or data to be destroyed or modified.

Responsibility for Content
Representatives of Wesleyan University publish institutional information in a variety of electronic forms. Such institutional information will normally be identified by a statement of the Certifying Authority publishing the information. A Certifying Authority is that University department or individual who certifies the accuracy of an electronic document and its appropriateness for the conduct of University business.

Users also publish information in electronic forms on Wesleyan equipment and/or over Wesleyan's networks. Wesleyan has no intention or opportunity to screen such private material and thus cannot assure its accuracy or assume any responsibility for this material. Any electronic publication provided on or over Wesleyan equipment and/or networks which is not identified by a Certifying Authority is the private speech of an individual user.

Threats and Harassment
Users may not use a University System to threaten or harass any person. A user must cease sending messages or interfering in any way with another user's normal use of University Systems if the aggrieved user makes a reasonable
request for such cessation, in the opinion of the cognizant Systems Administrator.

**Removal of Equipment or Documents**
Without specific authorization by the owner or System Administrator, users must not remove any University-owned or -administered equipment or documents from a University System.

**Unauthorized Computer Equipment**
Without specific authorization by the owner or System Administrator, users must not physically or electrically attach any foreign device (such as an external disk, printer, or video system) to a University System.

This restriction includes the unauthorized installation of any additional network-related or digital communications equipment (such as routers, hubs, or wireless access points) on the Wesleyan network.

**Violations**
Users must not conceal or help to conceal or "cover up" violations by any party.

Users are expected to report any evidence of actual or suspected violation of these policies to the Systems Administrator of the facility most directly involved. In case of doubt, the report should be made to the VP for Information Technology.

**University Rights**

**Personal Identification**
Users of University Systems must show identification including University affiliation upon request by a System Administrator or other University authority.

**Access to Data**
Users must allow systems administration personnel access to data files on University Systems for the purpose of making backups, diagnosing systems problems and investigating policy violations.

**Oversight Authority**
University staff are authorized to investigate alleged or apparent violations of University policy or applicable law involving University Systems using whatever means appropriate.
Enforcement Procedures
Systems Administrators are authorized by the University to investigate policy violations and apply temporary reduction or elimination of access privileges while the matter is under review. These temporary sanctions may apply to computing accounts, networks, University-administered computing rooms, and other services or facilities.

When a Systems Administrator believes it necessary to preserve the integrity of facilities, user services, or data, he or she may suspend any account or limit account privileges, whether or not the account owner (the user) is suspected of any violation. The System Administrator will attempt to notify the user of any such action.

When informed of copyright violations by the copyright holders or their representatives the University will comply with their requests to identify the individuals responsible and stop the illegal activity.

Depending on the role or status of the individual, authorization by the appropriate University Office will be sought before any access to electronic data occurs. In the case of students, the Vice President for Student Affairs would be consulted. For faculty, permission would be obtained from the VP for Academic Affairs and for staff, the appropriate University Officer would be notified.

A University User accused of a violation will be notified of the charge and will have an opportunity to respond to the University disciplinary body appropriate to the violator's status, before a final determination of any penalty.

In addition to discipline by Wesleyan University, users may be subject to criminal prosecution, civil liability, or both, for unlawful use of any University systems.