

Policy 1607

Information Technology Appropriate Use Policy

Responsible Office	Office of the Provost	Effective Date	9/26/00
Responsible Official	Provost of the University	Revised	1/13/10

Policy Sections	2
1607.1 Appropriate use of IT Systems.....	2
1607.2 Conditions of University Access.....	5
1607.3 Enforcement Procedures	6
1607.4 Policy Development	6

Scope

This Policy applies to all Users of IT Systems, including but not limited to University students, faculty, and staff. It applies to the use of all IT Systems. These include systems, networks, and facilities administered by ITS, as well as those administered by individual schools, departments, University laboratories, and other University-based entities.

Use of IT Systems, even when carried out on a privately owned computer that is not managed or maintained by Yale University, is governed by this Policy.

Policy Statement

The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic missions of the University in teaching, learning, research, patient care, and administration. In particular, this Policy aims to promote the following goals:

- To ensure the integrity, reliability, availability, and superior performance of IT Systems;
- To ensure that use of IT Systems is consistent with the principles and values that govern use of other University facilities and services;
- To ensure that IT Systems are used for their intended purposes; and
- To establish processes for addressing policy violations and sanctions for violators.

Reason for the Policy

Information technology ("IT"), the vast and growing array of computing and electronic data communications facilities and services, is used daily to create, access, examine, store, and distribute material in multiple media and formats. Information technology plays an integral part in the fulfillment of Yale University's research, education, clinical, administrative, and other roles. Users of Yale's IT resources have a responsibility not to abuse those resources and to respect the rights of the members of the community as well as the University itself. This Yale University IT Appropriate Use Policy (the "Policy" or "AUP") provides guidelines for the appropriate use of Yale's IT resources as well as for the University's access to information about and oversight of these resources.

Most IT use parallels familiar activity in other media and formats, making existing University policies important in determining what use is appropriate. Using electronic mail ("email") instead of standard written correspondence, for example, does not fundamentally alter the nature of the communication, nor does it alter the guiding policies. University policies that already govern freedom of expression and related matters in the context of standard written expression govern electronic expression as well. This Policy addresses circumstances that are particular to the IT arena and is intended to augment but not to supersede other relevant University policies.

For statements of other applicable University policies, consult the Undergraduate Regulations, the Graduate School Program and Policies, the Faculty Handbook, and the Personnel Policies and Practices Manual, as well as policy manuals and statements issued by each individual graduate and professional school. Yale's Department of Information Technology Services ("ITS") has promulgated policies that govern the use of various ITS Systems, such as Yale's NetNews and World Wide Web sites, the Pantheon system, and ITS email services. Other IT service providers at Yale have also adopted policies governing use of systems they manage. Please refer to postings available within each system to identify supplementary, tailored policies that also govern use of those systems.

Definitions

IT Systems: These are the computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by Yale University. For example, IT Systems include institutional and departmental information systems, faculty research systems, desktop computers, the University's campus network, and University general access computer clusters.

User: A "User" is any person, whether authorized or not, who makes any use of any IT System from any location. For example, Users include a person who accesses IT Systems in a University computer cluster, or via an electronic network.

Systems Authority: While Yale University is the legal owner or operator of all IT Systems, it delegates oversight of particular systems to the head of a specific subdivision, department, or office of the University ("Systems Authority"), or to an individual faculty member, in the case of IT systems purchased with research or other funds for which he or she is personally responsible.

Systems Administrator: Systems Authorities may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources.

Certifying Authority: This is the Systems Administrator or other University authority who certifies the appropriateness of an official University document for electronic publication in the course of University business.

Specific authorization: This means documented permission provided by the applicable Systems Administrator.

Policy Sections

1607.1 Appropriate use of IT Systems

Although this Policy sets forth the general parameters of appropriate use of IT Systems, faculty, students, and staff should consult their respective governing policy manuals for more detailed statements on permitted use and the extent of use that the University considers appropriate in light of their varying roles within the community. In the event of conflict between IT policies, this Appropriate Use Policy will prevail.

A. Appropriate Use. IT Systems may be used only for their authorized purposes -- that is, to support the research, education, clinical, administrative, and other functions of Yale University. The particular purposes of any IT System as well as the nature and scope of authorized, incidental personal use may vary according to the duties and responsibilities of the User.

B. Proper Authorization. Users are entitled to access only those elements of IT Systems that are consistent with their authorization.

C. Specific Proscriptions on Use. The following categories of use are inappropriate and prohibited:

1. **Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others.** Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters"

or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowing or reckless distribution of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

2. **Use that is inconsistent with Yale's non-profit status.** The University is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters. As a result, commercial use of IT Systems for non-Yale purposes is generally prohibited, except if specifically authorized and permitted under University conflict-of-interest, outside employment, and other related policies. Prohibited commercial use does not include communications and exchange of data that furthers the University's educational, administrative, research, clinical, and other roles, regardless of whether it has an incidental financial or other benefit to an external organization.
3. Use of IT Systems in a way that suggests University endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT Systems for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation with the University's General Counsel's Office.
4. **Harassing or threatening use.** This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another.
5. **Use damaging the integrity of University or other IT Systems.** This category includes, but is not limited to, the following six activities:
 - a) **Attempts to defeat system security.** Users must not defeat or attempt to defeat any IT System's security – for example, by "cracking" or guessing and applying the identification or password of another User, or compromising room locks or alarm systems. (This provision does not prohibit, however, ITS or Systems Administrators from using security scan programs within the scope of their Systems Authority.)
 - b) **Unauthorized access or use.** The University recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor this principle by neither seeking to obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. For example, a non-Yale organization or individual may not use non-public IT Systems without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-Yale organizations or individuals across the Yale network without specific authorization. Similarly, Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.
 - c) **Disguised use.** Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.
 - d) **Distributing computer viruses.** Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.
 - e) **Modification or removal of data or equipment.** Without specific authorization, Users may not remove or modify any University-owned or administered equipment or data from IT Systems.
 - f) **Use of unauthorized devices.** Without specific authorization, Users must not physically or electrically attach any additional device (such as an external disk, printer, or video system) to IT Systems.
6. Use in violation of law. Illegal use of IT Systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. Examples of such uses are: promoting a pyramid

scheme; distributing illegal obscenity; receiving, transmitting, or possessing child pornography; infringing copyrights; and making bomb threats.

With respect to copyright infringement, Users should be aware that copyright law governs (among other activities) the copying, display, and use of software and other works in digital form (text, sound, images, and other multimedia). The law permits use of copyrighted material without authorization from the copyright holder for some educational purposes (protecting certain classroom practices and "fair use," for example), but an educational purpose does not automatically mean that the use is permitted without authorization.

7. **Use in violation of University contracts.** All use of IT Systems must be consistent with the University's contractual obligations, including limitations defined in software and other licensing agreements.
8. **Use in violation of University policy.** Use in violation of other University policies also violates this AUP. Relevant University policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, as well as University, departmental, and work-unit policies and guidelines regarding incidental personal use of IT Systems.
9. **Use in violation of external data network policies.** Users must observe all applicable policies of external data networks when using such networks.

D. Free Inquiry and Expression. Users of IT Systems may exercise rights of free inquiry and expression consistent with the principles of the 1975 Report of the Committee on Freedom of Expression at Yale and the limits of the law.

E. Personal Account Responsibility. Users are responsible for maintaining the security of their own IT Systems 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 applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages.

F. Encryption of Data. Users are encouraged to encrypt files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. The University makes available software and protocols endorsed by the Information Security Office that provide robust encryption, as well as the capability for properly designated University officials to decrypt the information, when required and authorized under this Policy. Users encrypting information are encouraged to use only the endorsed software and protocols. Users who elect not to use endorsed encryption software and protocols on IT Systems are expected to decrypt information upon official, authorized request. (see section 1607.2, "Conditions of University Access," below.) A staff member may only encrypt with the permission of his or her supervisor.

G. Responsibility for Content. Official University information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document.

Users also are able to publish information on IT Systems or over Yale's networks. Neither Yale nor individual Systems Administrators can screen such privately published material nor can they ensure its accuracy or assume any responsibility for its content. The University will treat any electronic publication provided on or over IT Systems that lacks a Certifying Authority as the private speech of an individual user.

H. Personal Identification. Upon request by a Systems Administrator or other University authority, Users must produce valid University identification.

1607.2 Conditions of University Access

The University places a high value on privacy and recognizes its critical importance in an academic setting. There are nonetheless circumstances in which, following carefully prescribed processes, the University may determine that certain broad concerns outweigh the value of a User's expectation of privacy and warrant University access to relevant IT Systems without the consent of the User. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

A. Conditions. In accordance with state and federal law, the University may access all aspects of IT Systems, without the consent of the User, in the following circumstances:

1. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems; or
2. When required by federal, state, or local law or administrative rules; or
3. When there are reasonable grounds to believe that a violation of law or a significant breach of University policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or
4. When such access to IT Systems is required to carry out essential business functions of the University; or
5. When required to preserve public health and safety; or
6. **For Users who were members of the Yale faculty or staff: When the User's employment at Yale has ended and there is a legitimate business reason to access the User's IT Systems.**

B. Process. Consistent with the privacy interests of Users, University access without the consent of the User **pursuant to 1607.2 A (1) through (5)** will occur only with the approval of the Provost and cognizant Dean (for faculty users), the Vice President for **Human Resources** and Administration (for staff users), the Dean of Yale College or of one of the graduate or professional schools, as appropriate (for student users), or their respective delegates, except when an emergency entry is necessary to preserve the integrity of facilities or to preserve public health and safety. The University, through the Systems Administrators, will log all instances of access without consent **pursuant to 1607.2 A (1) through (5)**. Systems Administrators will also log any emergency entry within their control for subsequent review by the Provost, Vice President for Finance and Business Operations, dean, or other appropriate University authority. A User will be notified of University access to relevant IT Systems without consent pursuant to 1607.2 A (1) through (5). Depending on the circumstances, such notification will occur before, during, or after the access, at the University's discretion. **In the case of a former staff member, access without consent pursuant to 1607.2 A (6) must be approved by one of the former staff member's supervisors or their successors and no logging or notice is required. In the case of a former faculty member, access without consent pursuant to 1607.2 A (6) must be approved by the department chair or cognizant dean and no logging or notice is required.**

C. User access deactivations. In addition to accessing the IT Systems, the University, through the appropriate Systems Administrator, may deactivate a User's IT privileges, whether or not the User is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the User of any such action.

D. Use of security scanning systems. By attaching privately owned personal computers or other IT resources to the University's network, Users consent to University use of scanning programs for security purposes on those resources while attached to the network.

E. Logs. Most IT systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. All Systems Administrators are required to establish

and post policies and procedures concerning logging of User actions, including the extent of individually-identifiable data collection, data security, and data retention.

F. Encrypted material. Encrypted files, documents, and messages may be accessed by the University under the above guidelines. See 1607.1 - F, above.

1607.3 Enforcement Procedures

A. Complaints of Alleged Violations. An individual who believes that he or she has been harmed by an alleged violation of this Policy may file a complaint in accordance with established University Grievance Procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the Systems Authority overseeing the facility most directly involved, or to the University Information Security Office, which must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

B. Reporting Observed Violations. If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she may report any evidence to the Systems Authority overseeing the facility most directly involved, or to the University Information Security Office, which must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

C. Disciplinary Procedures. Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the Faculty Handbook, Staff Personnel Policies and Practices Manual, various student regulations (e.g., the Undergraduate Regulations for undergraduates, the relevant policy manuals for graduate and professional school students), and other applicable materials. Staff members who are members of University-recognized bargaining units will be disciplined for violations of this Policy in accordance with the relevant disciplinary provisions set forth in the agreements covering their bargaining units.

Systems Administrators and the Information Security Office may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, Systems Administrators and the Information Security Office are authorized to investigate alleged violations.

D. Penalties. Individuals found to have violated this Policy may be subject to penalties provided for in other University policies dealing with the underlying conduct. Violators may also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the Systems Administrator.

E. Legal Liability for Unlawful Use. In addition to University discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

F. Appeals. Users found in violation of this Policy may appeal or request reconsideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures.

1607.4 Policy Development

This Policy may be periodically reviewed and modified by the Provost of the University, who may consult with relevant University committees, faculty, students, and staff.

Procedures

[1607 PR1](#): Endorsed Encryption Implementation Procedure

Contacts

Subject	Contact	Phone
University Access & Enforcement	Provost of the University	432-4444
Information Technology Services	University Chief Information Officer	432-3262
Information Security	University Information Security Officer	432-1248

Revision History

2/21/2000, 9/26/2000, 1/13/03 (reformatting only), 1/13/2010

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.
