Acceptable Use of IT Resources (Network and Computing) Policy

Effective Date: July 1, 2007

Policy Statement
Columbia University requires that all individuals accessing University electronic information resources to abide by the standards of acceptable usage indicated within this policy.

The University is not responsible for information or materials residing on non-University systems or available over publicly accessible networks even if accessed via the University’s network. Such materials do not necessarily reflect the attitudes, opinions, or values of the University, its trustees, faculty, staff, or students.

The University reserves the right to modify or amend this policy and to limit or restrict the use of its electronic information resources at its sole discretion.

Reason for the Policy
Columbia University’s network and computing technology provides information, data, and communication services. Responsible use of electronic information resources is necessary to create and maintain an open community of responsible users based on mutual respect and cooperation, commitment to the integrity of resources and data, and compliance with all University policies and federal, state, and local statutes.

This policy defines acceptable usage of Columbia University network and computing resources.

Primary Guidance to Which This Policy Responds
This policy is established under the provisions of Columbia University’s Information Technology Security and Policy Program.

Responsible University Office & Officer
The office of Columbia University Information Technology Security is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Chief Information Security Officer (CISO) is the responsible officer.

Revision History
This policy was established in July 2007. The policy was updated in January 2011 to include prohibiting the use of University technology and resources for the purpose of intimidation and harassment of others.

Who is Governed by This Policy
This policy applies to all individuals who access, use, or control University electronic information resources. Those individuals covered include, but are not limited to staff, faculty, students, those working on behalf of the University, guests, tenants, visitors, and individuals authorized by affiliated institutions and organizations.

Who Should Know This Policy
Acceptable Use of IT Resources Policy - revised 01-11 (2).doc
All individuals governed by this policy should be familiar with it.

Exclusions & Special Situations
None

Policy Text
This policy establishes the expectations for all users of the University’s electronic information resources and data. It addresses the availability and integrity of resources in support of the University’s missions, codifies appropriate usage, establishes the need for users to respect the rights of others and to be in compliance with other University policies, policies of external networks and resources, and all applicable federal, state, and local statutes.

The University’s electronic information resources are provided to support the teaching, learning, clinical, and research missions of the University and their supporting administrative functions. Inappropriate use of these electronic information resources threatens the atmosphere for the sharing of information, the free exchange of ideas, and a secure environment for creating and maintaining electronic information resources.

Appendix A provides a partial list of relevant statutes regarding use of electronic information resources. Examples to assist with interpretation and administration of this policy are provided in Appendix B - “Examples of the Acceptable Use IT Resources” at the end of this document.

Responsibilities

General
• It is strictly prohibited to use University technology and resources for the purpose of intimidation and harassment of others.
• No University electronic information resource may be used for a purpose that violates University statutes or regulations or for an illegal or criminal purpose.
• Use of the University electronic information resources for commercial purposes, except where explicitly approved, are strictly prohibited. Prohibited uses include but are not limited to: development of programs, data processing or computations for commercial use, preparation and presentation of advertising material, or the running of a server connected to the University network.
• Many people use University systems and networks for daily work; therefore, obstructing this work by consuming excessive amounts of system resources or by deliberately crashing the machine(s) will not be tolerated. Before running large jobs on a shared system, perform due diligence by contacting the administrator of the system to determine if the job is permitted and how to minimize the impact. Network usage is continuously monitored and excessive use will be automatically restricted.
• Copying, storing, displaying, or distributing copyrighted material using University systems or networks without the express permission of the copyright owner, except as otherwise allowed under copyright laws, is prohibited. Under the Federal Digital Millennium Copyright Act of 1998, repeat infringements of copyright by a user can result in termination of the user's access to University systems and networks.
Network use

• The owner of any device connected to the network is responsible for the security of and traffic generated by that device. This includes any traffic, regardless of origin, that travels through such a device. A device initiating or transmitting an attack on other systems (e.g., having fallen victim to a virus, worm, or break-in) will be taken off the network immediately until it has been made secure.
• Unauthorized creation of any program, Web form, or other mechanism that asks for a Columbia user identity and password (e.g., UNI, CUNIX ID) is prohibited.
• No University network may be used as a vehicle to gain unauthorized access to other systems.

Computing use

• Immediately report any systems, which contain information classified as confidential, that have been compromised to CUIT Security using the “Contacts” information below. To preserve any evidence of tampering or misuse, do not use the system until a systems administrator has investigated the problem.
• Computer accounts provide access to personal and confidential data. Therefore, individual accounts cannot be transferred to or used by another individual and sharing accounts or passwords is not permitted.
• Each user is responsible for the proper use of his or her account, protecting data, and any activity performed via their user account. Therefore, choose strong passwords and safeguard them, ensure that file protections are set correctly, and review last logon status (if available) to ensure your user account was not compromised.
• Unauthorized attempts to escalate privileges on a University system, or access to any account or system not belonging to you are not permitted.
• Report possible security lapse on any University system or network to the system administrators.
• The system administrators conduct periodic security checks of University systems and networks, including password checks. Any user found to have an easily guessed or compromised password is required to change his or her password during next login.
• Any University system use by outside individuals or organizations requires special permission from the system's administrator and payment of fees to the University and to the appropriate software vendors where applicable.
• University computing facility use for playing computer games is strictly prohibited.
• Frivolous, disruptive, or inconsiderate conduct in computer labs or terminal areas is also strictly forbidden.

Privacy and information / data protection

• All private information (e.g., Social Security Numbers, credit information, passwords, etc) must be protected from unauthorized disclosure.
• Unauthorized attempts to read another person's protected files or gain access to their computer are prohibited.
• Local system administrators and providers of University electronic information resources and data have the additional responsibility of ensuring the integrity, confidentiality, and availability of the resources they are managing. Persons in these positions are granted
significant trust to use their privileges appropriately for their intended purpose and only when required to maintain the system. Any private information obtained in carrying out these duties must be treated in the strictest confidence.

- Local system administrators should not override files protections unless necessary in the course of their duties, and must treat the contents of those files as private information at all times.

Privacy Expectations
- User files or emails on central University systems are kept as private as possible.
- The University respects the privacy of individuals and does not routinely monitor the content of the information passing through its network, data stored on its servers, or posted by individuals not acting in an official capacity. However, to protect the integrity of its resources and the rights of all users, the University reserves the right to examine material stored on or transmitted through its resources if there is cause to believe that either a user violated the standards for acceptable computing use or a user gained unauthorized access to the University’s electronic information resources.
- There may be inadvertent inspection in the ordinary course of managing and maintaining the computer network and in carrying out other day-to-day activities. However, user files on central University systems are kept with utmost privacy.

Enforcement
Violations of these policies may result in the immediate suspension of computer account and network access pending investigation of circumstances and may lead to their eventual revocation. Serious violations will be referred directly to the appropriate University or outside authorities. Unauthorized use of University computing facilities is a criminal offense. The penalties may be as severe as suspension or dismissal from the University and/or criminal prosecution.

Definitions
Data is a stored collection of information that may include alphanumerics, words, sounds, symbols, or images.

Electronic Information Resources include data, networks, computers, and other devices that store or display data, communications devices, and software used on such devices.

Contacts
For questions or comments:
Columbia University Information Technology
Web: http://www.columbia.edu/cuit/support/
Email: security@columbia.edu
Telephone: 212-854-1919

Cross References to Related Policies
For CUIT Security Policies, see the University Administrative Policy Library, Information Security (CUIT) Responsible Office section:
http://policylibrary.columbia.edu/node_browser/nodes_by_category(term/7

Acceptable Use of IT Resources Policy - revised 01-11 (2).doc