

CU Home

Help



Search & Directories

 web
 people

Acceptable Use Policy

Your Responsibilities

Copyright Policy

Network Bandwidth

Domain Names

Mass E-mails

Safe Authentication

Information Security

Computer Security



COMPUTING, NETWORK, AND INFORMATION POLICIES

[Computing, Network & Information Policies](#) > **ACCEPTABLE USE POLICY**

[Print Page](#)

COLUMBIA UNIVERSITY COMPUTER AND ACCEPTABLE USE POLICY

Columbia University maintains certain policies with regard to the use and security of its computer systems, including the network. All users of these facilities are expected to be familiar with the policies and the consequences of violation as listed below.

COLUMBIA UNIVERSITY NETWORK SECURITY AND PRIVACY POLICIES

1. Unauthorized attempts to gain privileged access or access to any account or system not belonging to you on any University system are not permitted.
2. 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 except by using the methods documented for the Columbia secure server at <http://www.columbia.edu/acis/webdev/managing.html> or with the permission of the Deputy Vice President for Academic Information Systems or the Deputy Vice President for Administrative Information Services.
3. Computer and network accounts provide access to personal, confidential data. Therefore, individual accounts cannot be transferred to or used by another individual. Sharing accounts or passwords is not permitted.
4. Each user is responsible for the proper use of his or her account and any activity conducted with it. This includes choosing safe passwords, protecting them, and ensuring that file protections are set correctly.
5. Each system owner is responsible for the security of any system he/she connects to the network. A system seen to be attacking other systems, e.g. having fallen victim to viruses/worms, will be taken off the network, generally without notice, until it has been made secure. Security information is available at <http://www.columbia.edu/acis/security/>.
6. No University system or network may be used as a vehicle to gain unauthorized access to other systems.
7. Any user who finds a possible security lapse on any University system or network must report it to the system administrators. To protect your files and the system, don't attempt to use a system under these conditions until the system administrator has investigated the problem.
8. All users should be aware that the system administrators conduct periodic security checks of University systems and networks, including password checks. Any user found to have an easily guessed password will be required to choose a secure password during his or her next login process.
9. User files on central University systems are kept as private as possible. Attempts to read another person's protected files will be treated with the utmost seriousness. The system administrators will not override file protections unless necessary in the course of their duties, and will treat the contents of those files as private information at all times.

COLUMBIA UNIVERSITY NETWORK AND COMPUTING USAGE POLICIES

10. No University system or network may be used for any purpose or in a manner that violates University statutes or regulations or federal, state or local law.
11. Please keep in mind that many people use University systems and networks for daily work. Obstructing this work by consuming gratuitously large amounts of system

resources (disk space, CPU time, print quotas, network bandwidth) or by deliberately crashing the machine(s) will not be tolerated. Please cooperate by running large jobs on shared systems at off-peak hours and by using the "nice" command to lower the priority of CPU-intensive processes.

12. Use of any University system 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.
13. Use of University systems or networks for commercial purposes, except where explicitly approved, is strictly prohibited. Such prohibited uses include, but are not limited to, development of programs, data processing or computations for commercial use and preparation and presentation of advertising material.
14. Frivolous, disruptive, or inconsiderate conduct in computer labs or terminal areas is not permitted.
15. No University computing facility may be used for playing computer games.
16. 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 the copyright law, 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. See information on copyright at <http://www.columbia.edu/cu/help/copyright.html>.

COLUMBIA UNIVERSITY E-MAIL USAGE POLICIES

17. No e-mail may be sent or forwarded through a University system or network for purposes that violate University statutes or regulations or for an illegal or criminal purpose.
18. Electronic mail, like user files, is kept as private as possible. Attempts to read another person's electronic mail will be treated with the utmost seriousness. The University and its administrators of central e-mail systems will not read mail unless necessary in the course of their duties. Also, 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. On central systems e-mail that cannot be delivered to one or more addressees is directed to the system administrators for purposes of assuring reliable e-mail service, in most cases as "headers-only".
19. Users should be aware that their "deletion" of electronic information will often not erase such information from the system's storage until it is overwritten with other data and it may, in any case, still reside in the University's network either on various back-up systems or other forms, and even if erased, may still exist in the form of print-outs.
20. Nuisance e-mail or other online messages such as chain letters, obscene, harassing, or other unwelcome messages are prohibited.
21. Unsolicited e-mail messages to multiple users are prohibited unless explicitly approved by the appropriate University authority. See http://www.columbia.edu/cu/policy/mass_emails.html.
22. All messages must show accurately from where and from whom the message originated, except in the rare, specific cases where anonymous messages are invited.
23. The University reserves the right to refuse mail and other connections from outside hosts that send unsolicited, mass or commercial messages, or messages that appear to contain viruses to University or other users, and to filter, refuse or discard such messages.

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 of the policy will be referred directly to the appropriate University or outside authorities; unauthorized use of University computing facilities can be a criminal offense. The penalties may be as severe as suspension or dismissal from the University and/or criminal prosecution.

Rev 1.3.3 2003.01.08

THE EDUCOM CODE

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of

authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secrets and copyright violations, may be grounds for sanctions against members of the academic community.

1999.01.11

© Columbia University | Email based support