**Editor's Notes:**

POLICY TITLE: Carnegie Mellon University Computing Policy

DATE OF ISSUANCE: This policy was approved by the President's Council on May 16, 2003.

ACCOUNTABLE DEPARTMENTS/UNIT: Computing Services. Questions on policy content should be directed to the John Lerchey, Computer and Network Security Coordinator, x8-8170.

ABSTRACT: Sets forth university guidelines for use of computing resources.

RELATED POLICIES:
Appointment and Tenure Policy
Cheating and Plagiarism
Community Standards for Students
Conflict of Interest/Commitment
Copyright Policy of Carnegie Mellon University
Data and Computer Security (Confidentiality of Administrative Data)
Disciplinary Guidelines for Staff
Free Speech and Assembly and Controversial Speakers
Intellectual Property Policy
Policy Against Sexual Harassment
< /a>
Separation of Individual's and Institution's Interests

---

# CARNEGIE MELLON UNIVERSITY COMPUTING POLICY

## Policy Statement

The purpose of this policy is to set forth guidelines so that members of our community may use the campus network and computing facilities in ways that are responsible and respectful of privacy. This policy sets forth the university's expectations of acceptable behavior on the part of computer systems users at Carnegie Mellon by providing guidelines for appropriate use of computing and related communication systems and examples of inappropriate use. These standards of acceptable behavior also extend beyond the campus community into the Internet. Just as it is unacceptable to violate others' rights to privacy, property and resources within Carnegie Mellon, it is also unacceptable to violate those rights on systems that are not at Carnegie Mellon but are accessible through Carnegie Mellon's connection to the Internet.

This policy applies to all users of Carnegie Mellon computing systems, including students, faculty and staff, and any others granted the use of university computing resources. It applies to the use of all computing facilities owned, leased, operated or contracted by Carnegie Mellon University. As used in this policy, terms such as "computing," "computing/communications systems," "computing resources," etc., refer to all computers, communication systems, and peripherals, software, telephones and systems with similar functions, which are owned by Carnegie Mellon, or which utilize Carnegie Mellon infrastructure such as telephone lines or computer networks.

Although this policy does not attempt to deal specifically with legal issues, university members are responsible to act in compliance with the law, including any federal, state and local laws governing computer and telecommunications use, as well as all other applicable university policies.

## Privileges and

# Responsibilities

Every member of the Carnegie Mellon community who uses computing and related communications systems at Carnegie Mellon, or systems that belong to Carnegie Mellon or which rely on Carnegie Mellon's infrastructure has the responsibilities described in this policy. This includes members of the Carnegie Mellon community who have restricted privileges, such as alumni who may have electronic mail forwarding access, but no access to "login" resources. Individuals with personally-owned computers, but who rely upon the university network to connect those computers (either through an on-campus or remote network connection, such as Ethernet, wireless, dialup, DSL) are expected to abide by the policies set forth in this document. Personally-owned computers operating in stand-alone mode or networked through a non-university connection are not covered under this policy, but those users are encouraged to consult the usage policies set forth by their Internet Service Provider.

A fundamental premise of this policy is that anyone sharing computing resources with other individuals should behave as a reasonable, mature and ethical person. The user must recognize that computer systems and networks do not exist in some special rule-free environment; on the contrary, use of computers is a form of communication, and every component of a computing environment and every piece of information it contains belong to the university, the university community as a whole, or some individual or group within that community.

Access to Carnegie Mellon's computing resources is contingent upon being a member of the university community and adhering to university and Computing Services policies, guidelines and procedures, including this policy. Misuse may result in the loss of access and/or university disciplinary action. For some users and certain systems, access may be authorized by specific departments, research centers or other organizations affiliated with Carnegie Mellon. In such cases, any department- or group-specific policies and guidelines must be adhered to when using resources provided by the department or group. This is in addition to university policies and Computing Services guidelines and procedures.

Any user who suspects a violation of the University's computer use policies, or who has knowledge of potential vulnerabilities or security loopholes in a system or network at Carnegie Mellon, should immediately notify the Computer and Network Security Coordinator or abuse@andrew.cmu.edu.

## MAINTAIN THE SECURITY AND CONFIDENTIALITY OF YOUR ACCOUNT

Users assume personal responsibility for the use made of their computer accounts. This responsibility begins with selecting a secure password, and involves maintaining the confidentiality of that password and changing the password regularly in order to assure the continued security of your account. For guidance in selecting a secure password, see Managing Your Andrew Password. If you believe that someone has made unauthorized use of your account, you should change your password immediately and report the incident to the Computer and Network Security Coordinator or abuse@andrew.cmu.edu.

## RESPECT FOR OTHERS' PROPERTY AND PRIVACY RIGHTS

Users are responsible to respect copyright agreements and intellectual property ownership. Any material that is the work of another, whether explicitly copyrighted or not, should not be distributed by a user without appropriate acknowledgement and/or permission of the creator; unless permission has been granted by the owner of copyright protected materials, distribution of copyright protected material via the university network or computer systems is prohibited. So while the university has been granted permission by software vendors to distribute certain software packages via the network, it is not generally permissible for individual users to distribute that same software to others via the university network or computer systems. See the sections in this policy on Misuse and Inappropriate Behavior. While there may be cases in which property rights to particular programs, data, etc., are ambiguous or in dispute, the user must assume that any information not created by himself or herself belongs to someone else and must respect that person's privacy and property rights to that information. (In certain situations, even information created by the user may not belong to that user but rather to the university or others.) This policy is not intended to limit "fair use" as permitted under the Copyright Act and users having questions about whether a particular use constitutes a "fair use" may consult the General Counsel for advice.

IMPROPER/ILLEGAL COMMUNICATIONS

Any communications that would be improper or illegal on any other medium are equally so on the computer: libelous material, obscene messages, harassment, forgery, threats, etc. However, this is not intended to restrict the free expression of ideas. Communication conducted in accordance with the university policy on Free Speech and Assembly and Controversial Speakers and with the statement on Academic Freedom and Responsibility enunciated in the Appointment and Tenure Policy of Carnegie Mellon University will not be considered a violation of this policy. For further guidelines, see also the university policy on Separation of Individual's and Institution's Interests.

RESPONSIBLE SHARING OF RESOURCES

Where a resource such as memory, CPU time or access to network resources belongs to the whole community collectively, it must be shared.

It is unacceptable to make such excessive use of system or network resources that other users cannot obtain access. Examples include excessive use of CPU time during a period of heavy use on a timesharing system, excessive use of disk space on a system that does not limit such utilization, the use of an excessive amount of network bandwidth in an environment of networked computers, and any activity that makes a system unusable or significantly degrades performance for others. A novice user might be unaware that a particular action constitutes "excessive use" but, without doubt, once a system administrator makes him or her aware of the fact that such an action is unreasonable, that user will be held responsible for any further such infractions. If you are unsure whether your needs constitute excessive use, contact the system administrator. Similarly, if you need an unusual amount of disk space, CPU time or other resources, check with the system administrator to find out whether this use can be accommodated, rather than risk interfering with the work of others on the system.

RISKS OF DATA LOSS AND DATA PERSISTENCE

Although the university will make efforts to secure the network and university controlled servers from abuse and damage, it cannot guarantee against data loss by a student, faculty, member or staff, either on a university-operated or an individually-owned computer.

Users should know that even those files that they have "deleted" using the appropriate procedures in the application or operating system, may indeed be recoverable if they exist in a system backup file or other persistent form. If the university is asked to recover such data by subpoena, it must cooperate, and data that the user believes to have been destroyed may be recovered in the process.

PERSONAL USE

While the university makes computer resources available primarily to achieve its goals of education and research, and for administrative activities, it realizes the need to encourage the personal use of computing for the convenience of the campus community. Thus, it is reasonable to allow the use of computing resources for computer mail, document preparation, personal or course Web page publication, or other activity that can facilitate convenience or enhance productivity, to the extent that the activity is within the limits described by Responsible Sharing of Resources. Any personal use of computing resources related to operating a personal business or commercial enterprise is prohibited unless permission to do so has been specifically granted by the provost or the provost's designee.

We do recognize the difficulty of distinguishing whether certain cases of "personal use" are allowable, such as activities that result in personal financial gain (e.g. checking stock prices online), relate to a commercial business (e.g. university-sponsored technology transfer efforts), or support (but do not constitute operating) a personal business (e.g. a student developing a business plan or a faculty member writing a report for a consulting engagement outside the university). In such cases, we rely on individuals to be responsible and judicious in the use of university's shared computing resources. In particular ensuring:

- appropriate use of resources (e.g. any such work is completed outside of university time and does not utilize shared resources such as CPU cycles or network bandwidth to a degree that adversely impacts academic or research activities);
- appropriate use of licenses (e.g. do not use software procured with academic use licenses for commercial applications or development, unless the license

explicitly permits such use);

- appropriate marketing (e.g. no creation of ".com" domains within Carnegie Mellon's "edu" domain, no advertising services and products using Carnegie Mellon email accounts, and no advertising using web pages on Carnegie Mellon servers (any server with a .CMU.EDU host name).

In cases of questionable personal use of resources, you may contact advisor+@andrew.cmu.edu to determine whether a particular activity is permissible.

We reserve the right to restrict personal use of university systems and networks by an individual or by the community at large, if the use of resources for such activities becomes excessive. If you need unlimited access to computer networks for private or business purposes, you can subscribe to a commercial service.

For information regarding the use of resources to produce intellectual property and profit from the development of such property see Carnegie Mellon University's Intellectual Property Policy and the Policy on Conflict of Interest/Commitment.

## Privacy

The user must presume that the contents of any other users' directory are private unless expressly designated otherwise, just as one would presume that the contents of someone's apartment or office are private. The only exceptions to this rule are: that in some environments, files such as "plan files" may be considered public even if the user has not expressly designated them as such; and that some services such as web pages and anonymous or "guest access" ftp services may be considered to be public, but only for those areas not protected by password and which are "obviously" public. An unprotected account or shared device (such as a shared disk on a networked computer) are not considered to be public unless the name or service expressly indicates that it is. In such cases, any files or other data which would appear to be private in nature, by virtue of the file name or data stored, even if "publicly accessible" should be considered to be private. The user accessing such files has a responsibility to ask the owner of the files or service if the files are intended to be publicly accessible before the user does more than a "cursory glance" sufficient to cause the question.

A user can explicitly grant access to his or her directories, files or to services run from his or her systems. However, users who issue general or vague invitations to browse through their files incur a special obligation to protect any material that they do not wish others to see. Indeed, all users are urged to maintain protection levels on their files consistent with the access they are actually willing to give to other users.

ACCESS TO FACULTY DATA

Electronic data on a faculty member's account, whether stored on a computer in the faculty member's office or elsewhere under the proprietary control of that faculty member, may not be examined, i.e., the contents of the data read by a person, without the faculty member's consent, except in cases of emergency or in response to a valid subpoena, search warrant, or order of a court. Posting of data by a faculty member on servers available to the public or to students shall be understood to imply consent, and electronic access given to specific parties by the faculty member will likewise imply consent for those parties to access permitted data. Emergencies may include, for example, but are not limited to, the death, incapacity or disappearance of the faculty member, or the search for and examination of files used for apparently malicious activity in an account which endangers the integrity of shared computers, the network, or other aspects of the university's computing infrastructure.

Only specifically designated individuals are permitted to determine what passes for an "emergency." Such individuals may be specifically designated, or may be designated by job position/description. All assignments for individuals or positions will be done by Provost or by a designate of the Provost.

Whenever possible and legally permissible, notification must be given to the faculty member whose data are subject to subpoena, search warrant, or order of court prior to compliance therewith, and, whenever possible and legally permissible, sufficient time must be allowed, before intrusion, to allow the faculty member to file a motion to quash. Information obtained from an examination warranted by an emergency cannot be used as evidence in University sanctions of

any faculty member, and cannot be released to the public, or to the university community or to public officials, except as such releases are essential to resolution of the emergency, or constitute evidence of a crime concealment of which would obstruct justice, and in the latter case release may only be to appropriate law enforcement officials. Any intrusion by an employee of the University into a faculty member's electronic data must be reported to the faculty member as soon as possible, and within five days of the event in writing both to the faculty member, if possible, and unless prohibited by order of court, and to an Ombudsman, who shall be a member of the regular faculty selected annually by the Nominating Committee of the Faculty Senate and who has been endorsed by majority vote of the Faculty Senate. The Ombudsman shall be a current or retired regular faculty member who holds no administrative appointment and is not a member of the Faculty Review Committee. The Ombudsman shall have authority to investigate whether an intrusion was warranted by the policy and, (i) shall inform the President and the affected faculty member of the Ombudsman's findings; (ii) where a violation of the policy is found, shall inform the Faculty Review Committee of the policy violation; and (iii) where appropriate, in the absence of the affected faculty member, to bring a grievance before the Faculty Review Committee. Violation of any aspect of this policy is a sanctionable offense.

For purposes of this section, the term "faculty" shall mean any person who is a member of the Faculty Organization as defined in Article III of the Constitution of the Faculty Organization.

ACCESS TO STAFF DATA

Electronic data a staff member's account, whether stored on a computer in the staff member's office or elsewhere under the proprietary control of that staff member, may not be examined, i.e., the contents of the data read by a person, without the staff member's consent, except in cases of emergency, in response to a valid subpoena, search warrant, order of a court, or by specific request by the staff members' supervisor for the purpose of accessing work-related electronic data. Posting of data by a staff member on servers available to the public or to members of the university shall be understood to imply consent, and electronic access given to specific parties by the staff member will likewise imply consent for those parties to access permitted data. Emergencies may include, for example, but are not limited to, the death, incapacity or disappearance of the staff member, or the search for and examination of files used for apparently malicious activity in an account which endangers the integrity of shared computers, the network, or other aspects of the university's computing infrastructure.

Only specifically designated individuals are permitted to determine what passes for an "emergency." Such individuals may be specifically designated, or may be designated by job position/description. All assignments for individuals or positions will be done by Provost or by a designate of the Provost.

Whenever possible and legally permissible, notification must be given to the staff member whose data are subject to subpoena, search warrant, or order of court prior to compliance therewith. Information obtained from an examination warranted by an emergency will not be released to the public, or to the university community or to public officials, except as such releases are essential to resolution of the emergency, or constitute evidence of a crime concealment of which would obstruct justice, and in the latter case release may only be to appropriate law enforcement officials. Any such findings may be reported to the staff member's supervisor, department head, or to Human Resources for appropriate investigation and action. Any intrusion by an employee of the University into a staff member's electronic data must be reported to the staff member as soon as possible, and within five days of the event via electronic mail unless prohibited by order of court, or due to a continuance of an ongoing investigation by the University. Violation of any aspect of this policy is a sanctionable offense.

When possible, staff members will be informed about the issuance of court orders, or other intrusions into their electronic data. In cases where a staff member believes that electronic data in their account has been inappropriately accessed by another staff member, the incident should be reported to Human Resources.

ACCESS TO STUDENT DATA

Electronic data stored in a student account, whether stored on a computer in the student's residence or elsewhere under the proprietary control of that student, may not be examined, i.e., the contents of the data read by a person, without the student's consent, except in cases of emergency or in response to a valid subpoena, search warrant, order of a court, or by order of the Office of the Dean of Student Affairs. Posting of data by a student on servers available to the public shall be understood to imply consent, and electronic access given to specific parties by

the student will likewise imply consent for those parties to access permitted data. Emergencies may include, for example, but are not limited to, the death, incapacity or disappearance of the student, or the search for and examination of files used for apparently malicious activity in an account which endangers the integrity of shared computers, the network, or other aspects of the university's computing infrastructure.

Only specifically designated individuals are permitted to determine what passes for an "emergency". Such individuals may be specifically designated, or may be designated by job position/description. All assignments for individuals or positions will be done by Provost or by a designate of the Provost.

Whenever possible and legally permissible, notification must be given to the student whose data are subject to subpoena, search warrant, or order of court prior to compliance therewith. Information obtained from an examination warranted by an emergency will not be released to the public, or to the university community or to public officials, except as such releases are essential to resolution of the emergency, or constitute evidence of a crime of concealment which would obstruct justice, and in the latter case release may only be to appropriate law enforcement officials. Any findings of potential wrongdoing unrelated to the original intent of the search, must be reported to the Office of the Dean of Student Affairs for appropriate investigation and action. Any intrusion by an employee of the University into a student's electronic data must be reported to the student as soon as possible, and within five days of the event via electronic mail to the student, if possible, unless prohibited by an order of the court or because of an ongoing investigation conducted by the University. Violation of any aspect of this policy is a sanctionable offense.

When possible, students will be informed about the issuance of court orders, or other intrusions into their electronic data, including the purpose of the search. In cases where a student believes that electronic data in their account has been inappropriately accessed by a staff member, the incident should be reported to Office of the Dean of Student Affairs.

Note: Removable media such as floppy disks, zip drives, tapes, or CDs in a faculty or staff office, or in a residence hall are not subject to search by Computing Services, though Computing Services will assist authorized law enforcement agencies or authorities to read data after they are obtained, at the agencies' or authorities' request.

PROTECTING CONFIDENTIAL INFORMATION

Users who maintain confidential information, such as records relating to employees or students, are responsible for following privacy-related policies and laws.

PROTECTING PERSONAL INFORMATION

As is described throughout this policy, data transmitted across the university network or stored on university systems may be accessed by others as a result of misuse by an individual, as an incidental result of the routine operation of the network and systems, or in response to a court subpoena or university investigation into suspected or alleged misuse. While complete privacy of personal data may not be possible, users who wish to ensure a higher degree of privacy for their data are encouraged to use encryption, PGP security, or other techniques to reduce the risk that others may access their data. For more information on these techniques, see various newsgroups (e.g. comp.security.pgp) or web references (e.g. comp.security.pgp FAQ).

## Misuse and Inappropriate Behavior

The following activities are expressly prohibited at Carnegie Mellon:

- Using a computer system without proper authorization granted through the University, college, or department management structure. Some activities such as "port scanning" are not expressly prohibited. However, if the target of such scanning requests that an individual or system stop performing such actions, the person or system performing the scans must stop scanning the target machine unless the scans are being carried out by a system administrator who has the authority and responsibility over the machine(s) being scanned or for the

network being used.

- Concealing your identity, or assuming the identity of another (e.g., by sending forged electronic mail). Note that some forms of electronic communication, such as browsing Web pages, passively "identify" users. Keeping your identity private either by not setting an identity in your browser or by using a Web-anonymizer in order to protect yourself from being put onto mailing lists is not a violation of this policy.
- Sharing your password or account with the specific exception of staff or faculty members allowing their support personnel to access their accounts in order to provide services appropriate to their job functions. Note that some policies for the accessing of specific systems or data (see Data and Computer Security, Confidentiality of Administrative Data) explicitly forbid the sharing of passwords used to access them, and that such restrictions for those specific systems override this policy.
- Using another person's computer account, userID, files, or data without appropriate permission, as described in the previous bullet (e.g. using an account found "logged in" on a cluster machine).
- Deleting or tampering with another user's files or with information stored by another user on any information-bearing medium (disk, tape, memory, etc.). Even if the user's files are unprotected, with the exception of files obviously intended for public reading, such as Web pages, it is improper for another user to read them unless the owner has given permission (e.g. in an announcement in class or on a computer bulletin board).
- Attempting to "crack" or guess other users' passwords. System administrators or those specifically designated by the administrator or owner of a system may attempt to crack passwords in order to test and enhance the security of the system. In cases where an individual or department "owns" machines which use password files controlled by another organization (e.g. Andrew machines or their like), the owner may not attempt to crack passwords without explicit permission by the owners of the password database.
- Obtaining passwords by other means, such as password capturing programs.
- Attempting to circumvent system security (e.g. breaking into a system or using programs to obtain "root" access), without the explicit permission of the owner of that system.
- Denying appropriate access to resources to other users (e.g. "ping flooding" another system, sending "mail bombs," or modifying a login file in order to cause a user to not be able to log in).
- Releasing programs such as viruses, Trojan horses, worms, etc., that disrupt other users, damage software or hardware, disrupt network performance, or replicate themselves for malicious purpose.
- Sending commercial solicitations via electronic mail (i.e. spamming) to individuals, or to newsgroups or mailing lists where such advertising is not part of the purpose of the group or list. (It is permissible to send a commercial solicitation to a "for sale" newsgroup, provided that the advertisement conforms to other policies and guidelines at Carnegie Mellon.)
- Any "mass mailing" which is solicitous in nature, unless the mailing is in the conduct of university business.
- Reselling of services based on the university network, such as web hosting, mailing services or the selling of shell accounts.
- Running a proxy server which results in inappropriate or unauthorized access to university materials to non-university members.
- Advertising commercial businesses or ventures on Web pages hosted by Carnegie Mellon, unless prior authorization has been granted.
- Using mail messages to harass or intimidate another person (such as by repeatedly sending unwanted mail or broadcasting unsolicited mail).
- Violations of any local, state or federal laws, such as the distribution of copyright-protected materials (e.g. the distribution of commercial software, music or films in electronic format without appropriate permissions by the owner, even if the user distributing the materials notifies others of their copyright status).
- Tampering with, willful destruction of or theft of any computer equipment, whether it belongs to the university or to an individual. Tampering includes any deliberate effort to degrade or halt a system, to tie up a system or to compromise the system/network performance. Willful destruction includes any deliberate disabling or damaging of computer systems, peripheral equipment such as scanners or printers, or other facilities or equipment including the network, and any deliberate destruction or impairment of software or other users' files or data.

- The unauthorized removal of university or another's computing equipment, which constitutes theft.

This list should not be considered to be complete or exhaustive. It should, however, serve as a set of examples of obviously inappropriate behaviors. If you are in doubt about the appropriateness of something that you want to do, contact the Computing Services Help Center at 8-HELP, or send mail to advisor+@andrew.cmu.edu and ask first.

# Enforcement

Inappropriate behavior in the use of computers is punishable under the general university policies and regulations regarding faculty, students and staff. The offenses mentioned in this policy range from relatively minor to extremely serious, though even a minor offense may be treated severely if it is repeated or malicious. Certain offenses may also be subject to prosecution under federal, state or local laws.

Appropriate disciplinary action depends not only on the nature of the offense, but also on the intent and previous history of the offender. The range of possible penalties includes reprimands, loss of computing privileges, course failures for students, disciplinary probation, suspension or dismissal from the university and/or criminal prosecution.

Offenses that are minor or appear to be accidental in nature are often handled in a very informal manner such as through electronic mail. More serious offenses will involve formal procedures pursued through the Division of Student Affairs for students, Human Resources and/or the hiring university department or administrative unit for staff, or the Faculty Review Committee for faculty.

## RESTRICTIONS OF PRIVILEGES DURING INVESTIGATIONS

During the course of an investigation of alleged inappropriate or unauthorized use, it may be necessary to temporarily suspend a user's network or computing privileges, but only after determining there is at least a prima facie case against the individual, as well as a risk to the university or it's computing resources if privileges are not revoked. In these cases, it is important to recognize that the restriction of network or computing privileges is intended to protect the system rather than to punish the individual. For example, if a computer account has been used to launch an attack on another system, that account will be rendered inactive until the investigation is complete. This is a necessary action taken to prevent further misuse and does not presume that the account holder initiated the misuse. Unsubstantiated reports of abuse will not result in the suspension of accounts or network access unless sufficient evidence is provided to show that inappropriate activity occurred. For example, if someone reports that their computer was "attacked" by a Carnegie Mellon system, the burden will be upon the complainant to provide sufficient data logs or other evidence to show that the incident did, indeed at least appear to be an attack.

## ADVERSE IMPACT ON SHARED SYSTEMS

The university reserves the right to discontinue communication with external systems that are known to harbor spammers or account crackers, despite the fact that this may restrict certain acceptable communications. When deemed necessary, this action will be taken to protect the security and safety of our systems. Similarly, there may be cases where a particular service or activity on a given University system will, by the very nature of its legitimate operation, tend to generate attacks from other Internet sites. If these attacks are frequent and severe enough to cause service interruptions for larger parts of the campus community, it may be necessary to temporarily or permanently remove these systems from the campus network. In cases where such an action is deemed necessary, network administrators will work with the maintainers of the system to identify alternative methods of network access. In cases where the university restricts access to external sites or removes network access for internal sites, the purpose of the action is to maintain the security and reliability of the computer systems and networks rather than to punish an individual or a site, or to restrict the free expression of ideas.

# Contact

Questions concerning this policy or its intent should be directed to John Lerchey, Computer and Network Security Coordinator, x8-8170.