Institute Policy

Institute Policy on Acceptable Use of Electronic Information Resources

Caltech provides electronic information resources (including, but not limited to, computers, computer accounts and services, networks, software, electronic mail services, electronic information sources, video and voice services, servers, web pages, and related services) to assist members of the Institute community in the pursuit of education and research. This policy, in conjunction with other applicable Caltech policies, sets forth the acceptable use of all Caltech electronic information resources owned or managed by Caltech, and describes the rights and responsibilities of the Institute and of faculty, staff, students, and other members of the Institute community with respect to use of these resources.

Electronic information resources are intended to be used to carry out the legitimate business of the Institute, although some incidental personal use is permitted. Faculty, staff, students, and other members of the Institute community ("users") who use campus electronic information resources should be guided by the Institute's Honor System, which prohibits any member of the Institute community from taking unfair advantage of any other. In addition, users who use the Institute's electronic information resources assume responsibility for their appropriate use and agree to comply with all relevant Institute policies and all applicable local, state, and federal laws.

Users of Institute electronic information resources may not use these resources for inappropriate or unauthorized purposes. Some examples of inappropriate use are:sending a communication or using electronic information resources, including web pages, that discriminate against or illegally harass, defame, offend, or threaten individuals or organizations, or to engage in other illegal conduct or conduct that violates Institute policy;

- destruction of or damage to equipment, software, or data belonging to others;
- disruption or unauthorized monitoring of electronic communications;
- interference with use of Institute systems;
- violations of computer security systems;
- unauthorized use of accounts, access codes, or identification numbers;
- use of facilities in ways that intentionally impede the legitimate computing activities of others;
- use of facilities for commercial purposes;
- use for political or lobbying activities that jeopardize the Institute's tax exempt status and, therefore, violate Institute policy;
- violation of copyrights, software license agreements, patent protections and authorizations, or protections on proprietary or confidential information;
- unauthorized use of Caltech's trademarks;
- violating copyright laws by downloading and sharing files;
- violations of privacy;
- academic dishonesty;
- sending chain mail;
- spamming;
- intrusion into computer systems to alter or destroy data or computer programs (e.g., hacking or cracking); or
- sending communications that attempt to hide the identity of the sender or represent the sender as someone else.

Password capabilities and other safeguards are provided to members of the Caltech community in order to safeguard electronic messages, data, files, and other records (including computer files and records, electronic mail, and voice mail) from unauthorized use. In addition, the Institute will routinely follow up on systems and/or accounts that appear to be compromised or are in the process of being compromised. However, these safeguards are not intended to provide confidentiality from the Institute with respect to personal messages or files stored on Institute systems. Electronic information resources are Institute property. Users should not have an expectation of privacy with respect to their use of Institute electronic information resources or data, files, or other records generated, stored, or maintained on Institute resources.

The Institute may routinely examine network transmission patterns such as source/destination, address/port, flags, packet size, packet rate, and other indicia of traffic on the servers. While the Institute will not, as a routine matter,

review the content of electronic messages or other data, files, or records generated, stored, or maintained on Institute electronic information systems, the Institute retains the right, within its discretion, to inspect, review, or retain the content of electronic messages and other data, files, or records generated, stored, or maintained by users at any time without prior notification, for legitimate Institute reasons. These legitimate reasons include, but are not limited to, responding to lawful subpoenas or court orders, investigating misconduct and determining compliance with Institute policies, and locating electronic messages, data, files, or other records. Users should also understand that electronic messages, data, files, and other records generated, stored, or maintained on Institute electronic information systems may be electronically accessed, reconstructed, or retrieved even after they have been deleted. Institute access to the content of electronic mail, data, files, or other records generated, stored, or maintained by any member of the Caltech community may only be requested 1) by the provost for faculty; 2) by the associate vice president for human resources for employees; and 3) by the vice president for student affairs for students. In all cases, Institute access requires prior consultation with the Office of the General Counsel.

The use of Institute electronic information resources is a privilege, not a right, and the Institute may revoke this privilege, or decline to extend this privilege, at any time. Inappropriate use of Institute resources may result in administrative discipline up to and including separation from the Institute. Suspected illegal acts involving Institute electronic information services may be reported to state and federal authorities, and may result in prosecution by those authorities. Any questions concerning the appropriate use of any of the Institute's electronic information resources or relevant Institute policies should be directed to the provost, the chief information officer, the associate vice president for human resources, the dean of students, or the dean of graduate studies.

(For a signed copy of this policy, please refer to the PDF version of this document.)