Caltech 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, cellular phones 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 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 the use of these resources.

Electronic information resources provided by Caltech 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 Caltech's electronic information resources should be guided by the Caltech Code of Conduct. Users assume responsibility for the appropriate use of the Institute's electronic information resources and agree to comply with all relevant Institute policies and all applicable local, state, and federal laws. Examples of inappropriate or unauthorized use of the Institute's electronic information resources include:

- sending a communication or using electronic information resources, including web pages, that Illegally discriminate against, harass, defame, or threaten individuals or organizations;
- engaging in 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 that intentionally impedes the legitimate computing activities of others;
- use 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;
- downloading, viewing, and/or sharing of materials in violation of the Institute's policy regarding Unlawful Harassment, including Sexual Misconduct (http://www.hr.caltech.edu/services/policies);
- 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.

This policy will not be construed or applied in a manner that improperly interferes with employees' rights under the National Labor Relations Act.

Caltech's electronic information resources are Institute property and users should not have an expectation of privacy with respect to their use of these resources or any of the data, files, or other records generated by, stored or maintained on them. Password capabilities and other safeguards are provided to users in order to safeguard electronic messages, data, files, and other records (including computer files and records, electronic mail, and voice mail) from unauthorized use. These safeguards are not intended to provide confidentiality from the Institute with respect to personal messages or files stored on electronic information resources owned and managed by Caltech.

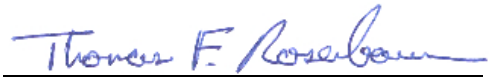
In order to protect the integrity of its electronic information resources, the Institute routinely monitors and examines network transmission patterns such as source/destination addresses/ports, flags, packet size, packet rate, and other indicators of traffic on its servers, which may at times include full packet capture. Caltech does not routinely capture or examine the content of electronic mail messages. The Institute will follow up on any system and/or account that appears to be compromised or is in the process of being compromised.

Caltech typically does not review the content of electronic messages or other data, files, or records generated, stored, or maintained on its electronic information resources; however, it retains the right to inspect, review, or retain the content of any such messages, data, files, and records at any time without prior notification. Any such action will be taken for reasons the Institute, within its discretion, deems to be legitimate. These legitimate reasons may include, but are not limited to, responding to lawful subpoenas or court orders; investigating misconduct (including research misconduct); determining compliance with Institute policies and the law; and locating electronic messages, data, files, or other records related to these purposes. Users must therefore understand that any electronic messages, data, files, and other records generated by, stored, or maintained on Institute electronic information resources may be electronically accessed, reconstructed, or retrieved by the Institute 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 user for reasons such as those described in the previous paragraph must be authorized as follows: (1) by the Provost for any situations that require access to electronic materials

associated with faculty and other academic personnel; (2) by the vice president of administration and chief financial officer for staff and postdoctoral scholars at campus or the JPL director for human resources for employees and postdoctoral scholars at JPL; (3) by the vice president for student affairs for students; or (4) by the general counsel for the purposes of complying with legal process and requirements or to preserve user electronic information for possible subsequent access in accordance with this policy. In all cases, the Office of the General Counsel should be consulted prior to making a decision on whether to grant access. In the case of a time-critical matter, if the authorizing official is unavailable for a timely response, the general counsel may authorize access.

In conclusion, 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 resources may be reported to state and/or 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 general counsel, the chief information officer, the associate vice president for human resources, the JPL director for human resources, the dean of undergraduate students, or the dean of graduate studies.



Thomas F. Rosenbaum
President