Caltech INSTITUTE POLICY

Acceptable Use of Electronic Information and Computing Resources

Caltech provides electronic information and computing resources (including, but not limited to, computers, computer accounts and services, networks, software, electronic mail services, electronic collaboration and communication platforms, electronic information sources, video and voice services, servers, websites, mobile devices, and related services) to assist members of the Caltech 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 (including those operated by third parties for Caltech, such as accounts or other computing services issued by third-party services for Caltech) (collectively, "**Caltech IT resources**") and describes the rights and responsibilities of Caltech and faculty, staff, students, postdoctoral scholars, visitors and guests and other members of the Caltech community.

Caltech IT resources are intended to be used to carry out the legitimate business of Caltech, although some reasonable incidental personal use is permitted. Incidental personal use must not violate any laws, Caltech's policies, including restrictions on political or outside commercial activities, or the safety, security, privacy, reputational, and intellectual property rights of others. Caltech is not responsible for any loss or damage incurred by an individual that results from personal use of Caltech IT resources.

Faculty, staff, students, postdoctoral scholars, visitors and guests and other members of the Caltech community ("users") who use Caltech's electronic information resources should be guided by the Caltech Code of Conduct. Passwords and other authentication mechanisms or devices issued to users are for their use only and are not to be shared with others. Users assume responsibility for the appropriate use of Caltech IT resources and agree to comply with all relevant Caltech policies and all applicable local, state, and federal laws. Examples of inappropriate or unauthorized use of Caltech IT resources include, but are not limited to:

- sending a communication or using electronic information resources, including websites, collaboration and communication platforms and social media sites to illegally discriminate against, harass, defame, or threaten individuals or organizations;
- sending communications that are threatening or that may constitute stalking under Caltech's policies regarding Violence Prevention or Sex Discrimination policies;
- engaging in illegal conduct or conduct that violates Caltech policy;
- collecting, distributing, or publishing, by means of an electronic communication device, another individual's personal identifying information or private or confidential information for purposes that are in violation of the law, including with the intent to cause fear, injury, or harassment (commonly referred to as "doxxing");

- destruction of, damage to, or malicious tampering with equipment, software, or data belonging to Caltech or to others;
- disruption, interception, or unauthorized monitoring of electronic communications;
- interference with use of Caltech systems;
- bypassing or otherwise tampering with computer security systems;
- unauthorized use of accounts, access codes, passwords, or identification numbers;
- use that intentionally impedes the legitimate computing activities of others;
- use for commercial purposes;
- use for cryptocurrency mining or any other personal profit-generating activities;
- use for political or lobbying activity that jeopardizes Caltech's tax-exempt status and violates Caltech's Political Activities Guidelines;
- violation of third-party intellectual property rights, including rights protected under patent, trademark, and copyright laws;
- downloading, posting, or sharing copyrighted materials, or any other unauthorized use or distribution of copyrighted materials;
- violation of software license terms;
- unauthorized use of Caltech's trademarks;
- unauthorized disclosure of proprietary or confidential information;
- violations of privacy;
- academic dishonesty;
- sending social media chain mail, spam, or other junk messages;
- fraudulent activity using Caltech IT resources;
- downloading, viewing, and/or sharing of materials in violation of Caltech's policies regarding Unlawful Harassment and Abusive Conduct and Sex Discrimination;
- unauthorized intrusion into computer systems;
- unauthorized security testing or scanning of Caltech IT resources or of another entity;
- sending communications that attempt to hide the identity of the sender or represent the sender as someone else;
- altering or disabling security devices or security configurations on IT assets;
- encrypting data or systems using cryptography that has not been reviewed and approved by Caltech; or
- use of generative AI and large language model tools in a manner that is inconsistent with Caltech's Guidance on the Use of Generative AI and Large Language Model Tools.

Caltech will apply this policy consistent with applicable requirements under the laws and regulations governing Caltech's operations. This policy will not be construed or applied in a manner that improperly interferes with employees' rights under the National Labor Relations Act.

Caltech IT resources are Caltech property or licensed by Caltech for Caltech's use. Users of Caltech IT resources 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.
For cybersecurity and other lawful purposes, Caltech may collect, store, and analyze information on both of the following: (1) any and all use of Caltech's electronic information resources and (2) any data or communications transmitted to or from, received or printed from, or created, stored, accessed, or recorded on Caltech's electronic information resources. This is true regardless of the labeling of the data, the use of encryption, the deletion of the data or communications, or any other factor.

Users of Caltech computing resources and information should understand the sensitivity level of the resources under their control and provide appropriate protection to both systems and data. Password capabilities and other authentication measures are provided to users in order to safeguard electronic messages, data, files, and other records (including computer files and records, electronic mail, and voicemail) and computing equipment from unauthorized use. These safeguards are not intended to provide confidentiality from Caltech monitoring with respect to personal messages or files stored on electronic information resources owned or managed by Caltech.

While Caltech does not routinely examine the content of electronic mail or communication messages or otherwise monitor individual usage, it does routinely monitor the normal operation of computing and networking resources, including network activity patterns, system logs, general and individual usage patterns, and other indicia necessary to ensure the integrity and stability of its electronic information resources.

Caltech will investigate suspected abuse, misuse, or compromise of its resources, systems, and services. Any user found to have violated this policy may be subject to disciplinary action, up to and including loss of administrative rights or network/system access, termination of employment, student expulsion, or being permanently excluded from Caltech-controlled premises.

Caltech retains the right to inspect, review, or retain the content of electronic messages or other data, files, or records generated, stored, or maintained on Caltech IT resources at any time without prior notification. Any such action will be taken for reasons Caltech, 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 Caltech 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 Caltech IT resources may be electronically accessed, reconstructed, or retrieved by Caltech even after they have been deleted.

Caltech personnel who wish to access the content of electronic mail, data, files, or other records generated, stored, or maintained by any user must request authorization as follows: (1) from the provost for any situations that require access to electronic material associated with faculty and other academic personnel; (2) from the associate vice president for human resources for staff and postdoctoral scholars at campus or the JPL director for human resources for employees and postdoctoral scholars at JPL; (3) from the vice president for student affairs for students; or (4) from the general counsel for the purposes of complying with legal processes 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 deciding 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. Users of Caltech IT resources are advised that some authorizations already have been granted. For example, the Caltech information security team has certain authority to monitor Caltech IT resources for cybersecurity purposes.

In conclusion, the use of Caltech electronic information resources is a privilege, not a right, and Caltech may revoke this privilege or decline to extend this privilege at any time.

Suspected illegal acts involving Caltech electronic information resources may be reported to governmental authorities and may result in prosecution by those authorities. Any questions concerning the appropriate use of any of Caltech's electronic information resources or relevant Caltech 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.

Report any suspected security incident or violation via email (security@caltech.edu) or, at JPL, by calling the JPL Helpdesk (4-HELP) or via email (abuse@jpl.nasa.gov).

Thomas F. Rosenbaum
President

Related Policies:

- Nondiscrimination and Equal Employment Opportunity Policy
- Sex Discrimination Policy
- Unlawful Harassment and Abusive Conduct Policy
- IMSS Security Policies
- Caltech Network Policy
- Confidentiality of Private Information Policy
- Vulnerability Scan Policy
- DMCA Infringement Policy
- Safeguarding Export Controlled Data Policy
- Email Policies
- Political Activities Guidelines
- Guidance on the Use of Generative AI and Large Language Model Tools