Policies

Cornell University Computing Policies

Users of Cornell University's IT resources are subject to local, state, and federal laws, as well as University IT policies, available online at http://www.it.cornell.edu/policies/university

Violations of policy may be prosecuted under the Campus Code of Conduct or the Code of Academic Integrity. The network is a Cornell University resource and Cornell IT may restrict any person's access to its resources with prior notice.

Security

Users of the Cornell network are responsible for the security of their computer and other networkable devices. See http://www.it.cornell.edu/security/computer .

The IT Security Office may monitor campus networks for systems showing signs of infection or compromise. Systems displaying serious vulnerabilities or problematic behavior may have their network access restricted or denied until the issue has been resolved.

Device Registration

University Policy 5.7 Network Registry requires that any computer or other networkable device connected to the Cornell network (wired or Wi-Fi) must be registered.

Data Collection by Cornell

Cornell IT collects data about network usage for security, performance, troubleshooting, and billing. Data collection is in compliance with *University Policy 5.1 Responsible Use of IT Resources.*

CNF Addendum

Faculty, researchers, staff, and visitors will operate under the guidelines and requirements described by Cornell University IT policies and procedures.

Computer abuse is a violation of university policy, and may subject the abuser to various disciplinary actions from CNF management, the campus judicial system, and legal authorities. Abuses of the computers at CNF will have the same results as violations of CNF safety rules ranging from denial of access to the computers for a period of time to permanent exclusion from the facility. Note that this policy covers ALL computers at CNF, from the networked systems to the individual computer workstations. Computer abuse includes, but is not limited to:

- Using CNF computer systems or networks without proper authorization, or for unauthorized purposes, including using or attempting to use an account not issued to you;
- Tampering with or obstructing the operation of the CNF computer systems or networks, or attempting to do so;
- Inspecting, modifying, distributing, or copying software or other data (whether this is system software, data, or files of another user) without authorization, or attempting to do so;
- Supplying false or misleading information or identification in order to access CNF's computer systems, or attempting to do so.

A longer description of abuse may be found in "Cornell University Policy Regarding Abuse of Computers and Network Systems" at: http://www.it.cornell.edu/policies/university/privacy/abuse