

Housing Services Internet and UCSF Network Use Agreement

UCSF's Internet and network resources are designed to facilitate the sharing of knowledge and information. This enhances and supports the educational and research experience of all UCSF affiliates. In partnership with ITS-Enterprise Network Services (ITS-ENS), Housing Services provides Mission Bay and 145 Irving Street tenants access to the Internet and the UCSF Network through data ports in each apartment. This access is a benefit of living at Mission Bay and 145 Irving Street but not a right. In order to ensure all UCSF affiliates can fully enjoy the services that access to this network provides, responsible use of this resource is of paramount importance.

As a primary leaseholder with access to the Internet and UCSF network, I agree to the following:

- 1.) Access to the Internet and UCSF network is provided for educational, research, and personal use, provided such use does not interfere with University operations, including the overall performance of the network.
- 2.) The University cannot guarantee complete electronic security or privacy for personal computing. It is important that each individual take reasonable security and privacy precautions to protect their computer and the network. At a minimum, all computing devices should have current Anti-virus and Anti-Spyware software, a host based firewall, and encryption software if ePHI or confidential information is stored locally. Enterprise Information Security (EIS) advises against storing any ePHI or confidential information on the local machine.
- 5.) I will not misuse the Internet or UCSF Network in any way. Examples of misuse include but are not limited to:
 - A.) **Installation an/ or operation of a wireless network access device without the prior written consent of ITS-ENS.**
 - B.) Installation and/ or operation of a multi-port network access device (e.g. hubs).
 - C.) Unauthorized operation of a general use file server, web server or any other multi-user system.
 - D.) Using electronic mail to harass others.
 - E.) Using the network to gain unauthorized access to any computer systems or accounts.
 - F.) Violating copyright laws by sharing copyrighted material (songs, movies, software, etc.) with others without the explicit permission of the copyright holder.
 - G.) Attempting to bypass any network security systems.
 - H.) Using excessive bandwidth and thus degrading the efficiency of the network.
 - I.) Knowingly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
 - J.) Using UCSF network resources for commercial purposes.
 - K.) Sending chain letters, advertisements, or solicitations of any type. Sending mass mailings to individuals who have not expressly agreed to be contacted in this manner.
 - L.) Masking the identity of an account or machine. Assuming the identity of another network user without their permission.
 - M.) Modifying network wiring.
 - N.) Non-compliance with UCSF's IP addressing scheme.
 - O.) Failing to take standard precautions for securing your computer as outlined above.
 - P.) Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place an excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.
 - Q.) Maliciously using tools designed to check for computer system or network security vulnerabilities (commonly known as port scanning).
 - R.) Network degradation due to faulty equipment, configurations or systems.
 - S.) Suspicious network traffic.
 - T.) Using the network in any way to violate any federal, state, or local laws and/ or any activity in violation of the UC Electronic Communications Policy (see below)
- 6.) Campus network maintenance is performed on the third Sunday of every month from 12:01AM to 6:00AM. Maintenance announcements are delivered via the UCSF Admin-1 Listserv. During maintenance, network services may be available but are not guaranteed.
- 7.) I am responsible for knowing and abiding by all ITS-ENS policies and guidelines including the UC Electronic Communications policy, the UCSF Acceptable Use policy, and Enterprise Information Security policies. These policies can be viewed here:
<http://www.ucop.edu/ucophome/policies/ec/> <http://www.research.ucsf.edu/IT/ItoliciesAcu.asp>
<http://isecurity.ucsf.edu>
- 8.) Any violation of ITS-ENS policies or this agreement could result in immediate termination of network access with or without notice. Unauthorized access or use of the UCSF Network is prohibited and may be subject to criminal and civil penalties.

Any breaches or suspected breaches of information security controls with respect to UCSF information system resources must be reported immediately:

Incident Reporting Procedure
http://isecurity.ucsf.edu/content/pdfs/unscheduled_outage_process.pdf
- 9.) If there are other non-primary leaseholder tenants living in my apartment (examples include spouses and children), I am responsible for monitoring their access to the Internet and ensuring they are aware of and follow this and all UCSF computer use related policies. At no time will non-UCSF personnel utilize the UCSF VPN to access the UCSF Network.

Leaseholder's Name

Date