OAC: Weill Housing Network Policies

Cornell University has policies and codes that govern the use of university computers and networks. The Weill Housing Network (WHN) is part of the Medical Center network. The Office of Academic Computing (OAC) will provide supported network connections and user support to all registered users of this service. Basic network services provided to Medical College faculty and staff will be provided to WHN with some additional restrictions.

It is essential that you review the University’s responsible computer use policies at http://www.cornell.edu/Computer/responsible-use/index.html.

In addition, because the WHN is connected to the NYP Hospital’s network, it is important that you respect the Electronic Medical Records policy of the Medical College and the Hospital (available soon).

Below is an overview of some of the common issues not specifically covered in the responsible use policy that are unique to the WHN. If you have any questions please do not hesitate to send e-mail to: WHN@med.cornell.edu.

User Responsibility: Students are personally responsible for all use of their computers and network connections and will be held accountable for any violations that occur involving their computer or network connections. Students should only allow others to use their machine with the full understanding of the possible consequences of that action. (See below)

No Shared Connections: A network connection supplied by WHN is solely for the use of a single computer assigned to that connection. Connections may not be shared among multiple computers. WHN subscribers cannot use any mechanisms (either hardware or software) to provide network connectivity to non-subscribers. The use of hubs, switches, routers, wireless networks (i.e. AirPorts) and similar devices is prohibited.

IP Address Usage: WHN subscribers are assigned an IP address for use with their specific jack at their particular campus address. The use of any IP address other than that assigned by WHN is prohibited. Subscribers who need to change jacks or rooms must contact WHN in advance to receive their new IP address for that new location. Use of unassigned IP addresses can cause conflicts, possibly resulting in a disruption of service for the person assigned that address.

Hostnames: All WHN IP addresses have associated hostnames that are registered automatically after someone subscribes. They take the form of OAC Tag#WHN.MED.CORNELL.EDU (i.e. pc102345.WHN.MED.CORNELL.EDU)

Custom domain names and registration of WHN IP addresses with external hostname registration agencies are prohibited. In addition, the registration of ".COM" commercial hostnames to a WHN IP address is considered a violation of the Cornell University Policy Regarding Abuse of Computers and Network Systems which prohibits the use of computers connected to the campus network for commercial purposes.

Servers: Remote access to WHN attached computers for personal uses of the subscriber is supported. However, servers are not to be run on the WHN network without express permission of OAC (i.e. Remote Access, WWW, FTP, File Servers etc). Send requests to WHN@med.cornell.edu.
Users of WHN that utilize multi-user operating systems (e.g., Windows NT or Unix) have the added responsibility to maintain reasonable security (no anonymous access, maintaining accurate logs, etc.). Workstations with inadequate security are often used by hackers to gain access to other campus hosts. Any workstation involved in a break-in attempt or that is identified as creating network problems will be disconnected from the campus network immediately.

**Access Billing:** Cornell reserves the right to bill for any unauthorized use of a network connection. WHN is a for-fee service and anyone attempting to use the service without proper authorization will be billed for all usage and may be referred to the appropriate administrative unit.

University owned networks, including WHN, are governed by policies and codes as well as federal, state, and local laws, which place certain restrictions on their use. These include the operation of any commercial or for-profit enterprise or advertising is prohibited, along with any re-sale of access or services. Illegal activities – including, but not limited to, such practices as fraud, harassment, software piracy, and copyright infringement – are also prohibited. In addition, IP spoofing, packet sniffing, virus distribution, or any activity that disrupts the network are violations of Cornell computer abuse policies.

The university reserves the right to place limited restrictions on the use of network systems in response to complaints presenting evidence of violations of university policies or codes, or state or federal laws. Once evidence is established, computers involved in alleged violations may be disconnected from the network until the situation is resolved.

Again, if you have any questions or require any clarification of this policy, please do not hesitate to send e-mail to WHN@med.cornell.edu or contact the Office of Academic Computing. For further details on Cornell policies and codes, refer to http://www.cornell.edu/Computer/responsible-use/Index.html.