

UNC-Chapel Hill Data Network Acceptable Use Policy

Overview

The University of North Carolina at Chapel Hill's Network Acceptable Use Policy ("AUP") sets forth the standards by which all students, faculty, staff, and authorized guests (hereafter referred to collectively as "User(s)") may use the shared University of North Carolina at Chapel Hill network. The use of UNC-Chapel Hill's network resources including all electronic communication systems and equipment (hereafter referred to collectively as the "UNC-Chapel Hill Network") is a revocable privilege.

The UNC-Chapel Hill network is provided to support the University of North Carolina at Chapel Hill business and its mission of education, service, and research. Any other uses, including uses that jeopardize the integrity of the UNC-Chapel Hill Network, the privacy or safety of other Users, or that are otherwise illegal are prohibited.

By using or accessing the UNC-Chapel Hill Network, Users agree to comply with the Network AUP and other applicable UNC-Chapel Hill policies which may be implemented from time to time, as well as all Federal, state, local laws and regulations. Using and/or accessing the UNC-Chapel Hill Network without proper authorization is strictly prohibited.

I. Principles

General guidelines for acceptable use of the UNC-Chapel Hill Network are based on the following principles:

1. Users are expected to behave responsibly with respect to the UNC-Chapel Hill Network at all times.
2. Users are expected to respect the integrity and the security of the UNC-Chapel Hill Network.
3. Users are expected to behave in a manner consistent with UNC-Chapel Hill's mission and comply with all applicable laws, regulations, and UNC-Chapel Hill policies.
4. Users are expected to be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to use the UNC-Chapel Hill Network and show restraint in the consumption of shared resources.
5. Users are expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.

Users shall avoid unnecessary network traffic and interference with other users.

II. Prohibitions

The following activities are specifically prohibited:

1. Users may not attempt to disguise their identity, the identity of their account or the machine that they are using. Users may not attempt to impersonate another person or organization. Users may not appropriate the University of North Carolina at Chapel Hill's name, network names, or network address spaces.
2. Users may not attempt to intercept, monitor, forge, alter or destroy other Users' communications. Users may not infringe upon the privacy of other computers or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of the owner.
3. Users may not engage in actions that disrupt or interfere with the legitimate use by other Users of any computers and/or networks, including the UNC-Chapel Hill Network, that interfere with the supervisory or accounting functions of the systems, or that are likely to have such effects. Such conduct includes, but is not limited to: placing of unlawful information on the system, transmitting data or programs likely to result in the loss of an individual's work or system downtime, sending "chain letters" or "broadcast" messages to lists or individuals, or any other use that causes congestion of any networks or interferes with the work of others, i.e. spam.
4. Users may not distribute or send unlawful communications of any kind, including but not limited to threats of violence, obscenity, child pornography and/or harassing communications (as defined by law).
5. Users may not attempt to bypass network security mechanisms, including the UNC-Chapel Hill Network, without the prior express permission of the owner of that system. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent to such an attempt. The unauthorized scanning of the UNC-Chapel Hill Network is also prohibited.
6. Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permissions of the copyright holder. Information on the Digital Millennium Copyright Act can be found at: <http://www.copyright.gov/legislation/dmca.pdf> and the Copyright Act at: <http://www.copyright.gov/title17/>.
7. Users may not use the UNC-Chapel Hill Network for private business, commercial or political activities, fundraising, or advertising on behalf of non-UNC-Chapel Hill organizations, unlawful activities or uses that violate other University of North Carolina at Chapel Hill policies. Users may not extend or share the UNC-Chapel Hill Network.
8. Users may not violate any laws or ordinances, including, but not limited to, copyright, discrimination, harassment, and/or export controls. The University of North Carolina at Chapel

Hill may contact local or federal law enforcement authorities to investigate any matter at its sole discretion.

9. Users are not permitted to connect any network devices or systems (including but not limited to switches, routers, wireless access points, VPNs, and firewalls) without advance notice to and consultation with ITS Telecommunications at UNC-Chapel Hill (see <http://help.unc.edu/?id=3742> for a full description of the Network Infrastructure Policy in this regard).

III. Review and Penalties

In appropriate circumstances, the University of North Carolina at Chapel Hill reserves the right to review and/or monitor any transmissions sent or received through the UNC-Chapel Hill Network, at its sole discretion.

Penalties for violating the Network AUP may include restricted access or loss of access to the UNC-Chapel Hill Network, termination and/or expulsion from the University of North Carolina at Chapel Hill and in some cases, civil and/or criminal liability.

The University of North Carolina at Chapel Hill reserves the right to update or revise the Network AUP or implement additional policies in the future. Users are responsible for staying informed about UNC-Chapel Hill policies regarding the use of computer and network resources and complying with all applicable policies. ITS Networking shall provide notice of any such modifications or amendments by email to the UNC-CH Support and CTC mailing lists. Any such modification shall be effective immediately upon notice being provided regardless of whether subscriber actually reads such notice. The current version of this policy can be found at <http://help.unc.edu/?id=1672>.

IV. Additional IT Acceptable Use Policies

Additional policies related to the acceptable use of other IT systems and services at the University of North Carolina at Chapel Hill can be found at <http://help.unc.edu/?trail=1597>.

Dated 16 April 2007