Computer Acceptable Use Policy

UNC-Chapel Hill Network Acceptable Use Policy

from http://help.unc.edu/help/unc-chapel-hill-network-acceptable-use-policy/

I. Purpose

The University Network incorporates all electronic communication systems and equipment at the University of North Carolina at Chapel Hill (the "University"). This Network Acceptable Use Policy ("AUP") sets forth the standards by which all Users may use the shared University Network.

The University Network is provided to support the University and its mission of education, service, and research. Any other uses (other than permitted personal use as discussed below), including uses that jeopardize the integrity of the University Network, the privacy or safety of other Users, or that are otherwise illegal are prohibited. The use of the University Network is a revocable privilege.

By using or accessing the University Network, Users agree to comply with this AUP and other applicable University policies which may be implemented from time to time, as well as all federal, state, and local laws and regulations. Only Users are authorized to use and/or access the University Network.

The term "User" refers to any faculty, staff, or student associated with the University, as well as any other individual with access to computers or other network devices that have been approved by the Assistant Vice Chancellor for ITS Communication Technologies for connection to the University Network. This definition includes, but is not limited to, contractors, visitors, and temporary affiliates.

II. Principles

General requirements for acceptable use of the University Network are based on the following principles:

1. Each User is expected to behave responsibly with respect to the University Network and other Users at all times.
2. Each User is expected to respect the integrity and the security of the University Network.
3. Each User is expected to behave in a manner consistent with University's mission and comply with all applicable laws, regulations, and University policies.
4. Each User is 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 University Network and show restraint in the consumption of shared resources.
5. Each User is expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.
6. Each User is expected to cooperate with the University to investigate potential unauthorized and/or illegal use of the University Network.
7. Each User is expected to respect the security and integrity of university computer systems and data.

III. Prohibitions

A. Without limiting the general guidelines listed above, unless expressly agreed to by the Chief Information Officer, 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 likewise not misuse or appropriate the University's

name, network names, or network address spaces.

2. Users may not attempt to intercept, monitor, forge, alter or destroy another User's communications. Users may not infringe upon the privacy of others' computer or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of such other User.
3. Users may not use the University Network in a way that (a) disrupts, adversely impacts the security of, or interferes with the legitimate use of any computer, the University Network or any network that the University connects to, (b) interferes with the supervisory or accounting functions of any system owned or managed by the University, or (c) take action that is likely to have such effects. Such conduct includes, but is not limited to: hacking or spamming, placing of unlawful information on any computer system, transmitting data or programs likely to result in the loss of an individual's work or result in 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.
4. Users may not distribute or send unlawful communications of any kind, including but not limited to cyberstalking, threats of violence, obscenity, child pornography, or other illegal communications (as defined by law). This provision applies to any electronic communication distributed or sent within the University Network or to other networks while using the University Network.
5. Intentional access to or dissemination of pornography by University employees, temporary staff, contractors, or vendors is prohibited unless (1) such use is specific to work-related functions and has been approved the respective manager or (2) such use is specifically related to an academic discipline or grant/research project. This provision applies to any electronic communication distributed or sent within the University Network or to other networks while using the University Network.
6. Users may not attempt to bypass network security mechanisms, including those present on the University Network, without the prior express permission of the owner of that system. The unauthorized network scanning (e.g., vulnerabilities, post mapping, etc.) of the University Network is also prohibited. For permission to perform network scans, user must receive prior approval by calling 919-962-HELP and submitting a Remedy ticket to the Information Security Office.
7. Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permission of the copyright holder or as otherwise allowed by law. 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/. Additional information may be found on the home page of the University's Copyright Committee (http://library.unc.edu/scholcom/).
8. Except as allowed under the Personal Use Policy or the Policy on Use of University Resources in Support of Entrepreneurial Activities. Users may not use the University Network for private business, commercial or political activities, fundraising, or advertising on behalf of non-University organizations, unlawful activities, or uses that violate other University policies.
9. Users may not extend or share with public or other users the University Network beyond what has been configured accordingly by ITS Communication Technologies/Networking. Users are not permitted to connect any network devices or systems (e.g., switches, routers, wireless access points, VPNs, and firewalls) to the University Network without advance notice to and consultation with ITS Communication Technologies at the University (see https://help.unc.edu/help/data-network-infrastructure-policy/ for a full description of the Data Network Infrastructure Policy in this regard). To contact ITS Communication Technologies, users must call 919-962-HELP and submit a Remedy ticket to ITS Communication Technologies /Networking.
10. Users are responsible for maintaining minimal security controls on their personal computer equipment that connects to the University Network, including but not limited to: current antivirus software, current system patches, and strong passwords. For more detailed information on securing a personal computer or network device, go to http://help.unc.edu/ and search for the keywords "best practices".
11. Users may not violate any laws or ordinances, including, but not limited to, laws related to copyright, discrimination, harassment, threats of violence and/or export controls.

IV. Review and Penalties

A. The University reserves the right to review and/or monitor any transmissions sent or received through the University Network. University access to electronic mail on the University Network is permitted in accordance with the University's Policy on the Privacy of Electronic Information (http://policies.unc.edu/policies/electronic-privacy/). Access to other transmissions sent or received through the University Network may occur in the following circumstances:

1. in accordance with generally accepted, network-administration practices
2. to prevent or investigate any actual or potential information security incidents and system misuse, if deemed necessary by authorized personnel
3. to investigate reports of violation of University policy or local, state, or federal law

4. to comply with legal requests for information (such as subpoenas and public records requests)
5. to retrieve information in emergency circumstances where there is a threat to health, safety, or University property involved

B. Penalties for violating this AUP may include:

1. restricted access or loss of access to the University Network
2. disciplinary actions against personnel and students associated with the University
3. termination and/or expulsion from the University
4. civil and/or criminal liability

The University, in consultation with its legal counsel, may contact local or federal law enforcement authorities to investigate any matter at its sole discretion.

V. Policy Updates

The University reserves the right to update or revise this AUP or implement additional policies in the future. Users are responsible for staying informed about University policies regarding the use of computer and network resources and complying with all applicable policies. The University shall provide notice of any such modifications or amendments by email to the University community. 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://its.unc.edu/about-us/how-we-operate/.

VI. Additional IT Acceptable Use Policies

Additional policies related to the acceptable use of other IT systems and services at the University can be found at:

- Policy on the Privacy of Electronic Information: http://policies.unc.edu/policies/electronic-privacy/
- Personal Use Policy: http://financepolicy.unc.edu/policy-procedure/105-personal-use-policy/
- Policy on Use of University Resources in Support of Entrepreneurial Activities: http://research.unc.edu/offices/vice-chancellor/policies-issues/data_vcred_entrep_sp/
- Data Network Infrastructure Policy: https://help.unc.edu/help/data-network-infrastructure-policy/

Contacts

Subject	Contact	Telephone	FAX
Policy Questions	The University's Information Security Office	919-445-9393	919-445-9488
Report a Violation	The University's Information Security Office	919-445-9393	919-445-9488
Request Information Security Consulting	The University's Information Security Office	919-445-9393	919-445-9488

Last Updated: 8/19/2014