UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
UNC-Information Technology Services

POLICY

UNC-Chapel Hill Information Technology Acceptable Use Policy

Policy Statement

By using or accessing UNC-Chapel Hill's information technology systems or services ("IT," as more fully defined below), including connection of any device to any University network or information system. UNC-Chapel Hill Users agree to comply with this Acceptable Use Policy ("AUP") and other applicable University policies, as well as all federal, state, and local laws and regulations. Only Users in compliance with this AUP are authorized to use and/or access University IT.

I. Guiding Principles

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

1. Each User is expected to behave responsibly and in a manner consistent with the University's mission with respect to University IT and other Users at all times.

2. Each User is expected to respect the integrity and the security of University IT and data.

3. 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 University IT and show restraint in the consumption of shared resources.

4. Each User is expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.

5. Each User is expected to cooperate with the University to investigate potential unauthorized and/or illegal use of University IT.

II. Prohibitions

Without limiting the general guidelines listed above, unless expressly agreed to by the Chief Information Officer (CIO), the following activities are 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 engage in cyberstalking or 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 University IT in a way that (a) disrupts, adversely impacts the security of, or interferes with the legitimate use of any University IT, 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 store, display or disseminate unlawful communications of any kind, including but not limited to threats of violence, obscenity, child pornography, or other illegal communications. This provision applies to any electronic communication distributed or sent within University IT or to other networks while using University IT.

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 a User's supervisor/unit manager or (2) such use is for scholarly or medical purposes. This provision applies to any electronic communication residing on, distributed or sent using University IT, including to other networks while using University IT.

6. Users may not attempt to bypass network security mechanisms, including those present on University IT, without the prior express permission of the owner of that system. The unauthorized network scanning (e.g., vulnerabilities, post mapping, etc.) of University IT is also prohibited. For permission to perform network scans, user must receive prior approval from the Information Security Office by calling 962-HELP.

7. Users must not use University IT to violate copyright, patent, trademark, or other intellectual property rights. Examples of such violations would include engaging 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://www.lib.unc.edu/copyright/).

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 University IT for private business, commercial or political activities, fundraising, or advertising on behalf of non-University entities.

9. Users may not extend or share the University network with the public or other users 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 http://help.unc.edu/3742 for a full description of the Data Network Infrastructure Policy in this regard).

10. Users are responsible for maintaining security controls on their personal computer equipment that connects to University IT or that stores and processes University institutional information, according to the Information Security Controls Standard, available at http://its.unc.edu/about-us/how-we-operate/.

III. IT Security and Monitoring

The University may review and/or monitor any use of University IT. 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://www.unc.edu/campus/policies/elec_info.html). Review or monitoring of use of University IT may occur in the following circumstances if deemed necessary by authorized personnel:

1. in accordance with generally accepted, network-administration practices;

2. to prevent or investigate any actual or potential information security incidents and system misuse;

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); or

5. to retrieve information in emergency circumstances where there is a threat to health, safety, or University property involved

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

Purpose and Background

University IT comprises computers, mobile devices, ancillary equipment, software, services, including network and support services, and related resources at the University of North Carolina at Chapel Hill (the "University"). This IT Acceptable Use Policy ("AUP") sets forth the standards by which all Users may use University IT.

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

Audience

All Users of University IT.

Compliance

Penalties for violating this Policy may include restricted access or loss of access to University IT.

Failure to comply with this policy may put University information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Students who fail to adhere to this policy may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors, vendors, and others who fail to adhere to this policy may face termination of their business relationships with UNC-Chapel Hill.

Violation of this policy may also carry the risk of civil or criminal penalties.

Definitions

Hacking: Gaining unauthorized access to an information system.

Information Technology Systems and Services ("IT"): Any equipment or interconnected system or subsystem of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, mobile devices, ancillary equipment, software, services, including network and support services, and related resources.

Spamming: Electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

UNC-Chapel Hill Affiliate: UNC-Chapel Hill faculty, staff, students, retirees, contractors, distance learners, visiting scholars and others who require UNC-Chapel Hill resources to work in conjunction with UNC-Chapel Hill.

UNC-Chapel Hill User: Any UNC-Chapel Hill Affiliate, or other individual, including campus visitors, with access to University information technology systems or services.

Related Documents

Data Network Infrastructure Policy: http://help.unc.edu/3742

EPA Non-Faculty Employee Policies: http://hr.unc.edu/policies-procedures-systems/epa-non-faculty-employee-policies/

Faculty Handbook: http://facultyhandbook.unc.edu/

Graduate Student Handbook: http://handbook.unc.edu/

Personal Use Policy: http://financepolicy.unc.edu/105

Policy on the Privacy of Electronic Information:
http://www.unc.edu/campus/policies/elec_info.html

Policy on Use of University Resources in Support of Entrepreneurial Activities:
http://research.unc.edu/offices/vice-chancellor/policies-issues/data_vcred_entrep_sp/

SPA Employee Handbook: http://hr.unc.edu/policies-procedures-systems/spa-employee-policies/

UNC Information Security Controls Standard: http://its.unc.edu/about-us/how-we-operate/

Undergraduate Bulletin http://www.unc.edu/ugradbulletin/

For more detailed information on securing a personal computer or network device, go to help.unc.edu and search for the keywords “best practices”.

Contacts

Subject	Contact	Telephone	Online/Email
Policy Questions	Communication Technologies or Information Security Office	919-962-HELP	Help.unc.edu
Report a violation	Communication Technologies or Information Security Office	919-962-HELP	N/A

Document History

- Effective Date: April 7th, 1998 (19980407)
- Revised Date: February 18, 2016 (20160218), Vice Chancellor for Information Technology and Chief Information Officer. This document supersedes the previous Data Network Acceptable Use Policy and has expanded scope to cover all use of University IT.