Information Technology Acceptable Use Policy

Summary

All members of the University community who engage with any University information technology (including wireless or other networks) must adhere to this Acceptable Use Policy.

Body

Title

University of North Carolina at Chapel Hill Information Technology Acceptable Use Policy

Introduction

Purpose

The University of North Carolina at Chapel Hill (“UNC-Chapel Hill” or “University”) supplies Information Technology (IT) to support the University’s mission of research, education, and public service. University IT includes:

- Computers,
- Mobile devices,
- Other equipment,
- Software and software services,
- Internet connection and networking,
- IT support services, and
- IT-related resources at the University.

This IT Acceptable Use Policy ("AUP") sets rules for anyone using University IT.

Scope

Anyone using University IT.

Policy

Policy Statement

The use of University IT is a privilege that can be taken away. By using or accessing the University’s IT systems, networks, or services, you agree to follow this AUP. You also agree to follow other University policies, as well as all relevant federal, state, and local laws and regulations. Only people following this AUP may use or access University IT.

Other uses of University IT are not allowed unless an exception applies. Uses that can harm University IT other privacy or safety of other people, and illegal uses are prohibited.

I. Guiding Principles

Acceptable use of University IT is based on the following guiding principles:

1. Act responsibly toward other people and in ways that are consistent with the University's mission.
2. Protect the integrity and the security of University IT and data.
3. Be considerate of other people's needs. Try not to interfere with other people using University IT. Be aware of your use of shared resources.
4. Respect the rights and property of others including their privacy, confidentiality, and intellectual property.
5. Cooperate with the University to investigate potential unauthorized 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. Attempting to hide or change a person's identity, the identity of an account, or the device being used.
2. Impersonating another person or organization.
3. Misusing the University's name, network names, or network address spaces. Pretending to represent the University when that is not true.
4. Attempting to intercept, track, forge, change, or destroy another person's communications or data.
5. Engaging in cyberstalking or infringing on the privacy of others' computer or data. unless that person has given you clear permission before you do it.
6. Using University IT in a way that:
    a. Disrupts, harms the security of, or gets in the way of legitimate use of any University IT,
    b. Interferes with the administration or data protection of any system owned or managed by the University, or
    c. Is likely to have those effects. Examples include:
        - Hacking,
        - Spamming,
        - Putting unlawful information on any computer system,
        - Sending data or programs likely to cause the loss of a person's work or cause 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.
7. Storing, displaying, or sharing unlawful communications of any kind. Examples include threats of violence, obscenity, or child pornography. Illegal communications on, through, or starting from within University IT are not allowed. Accessing or sharing pornography using University IT is not allowed unless the use complies with law (including NCGS 134-805(d)) and such use:
    - is specific to job-related functions, such as scholarly research, cybersecurity, or medical purposes, and
    - has been approved by the person's supervisor or unit manager.
      OR
    - The use is by a non-employee Student,
    - is not otherwise unlawful,
    - and is not using a University device.
8. Trying to bypass network security tools unless someone responsible for that system has given you permission beforehand. Unauthorized network scanning (e.g., vulnerabilities, port mapping, etc.) of University IT is prohibited. The University's Information Security Office must approve all network scans. Call 919-962-HELP to request permission to perform network scans.
9. Using University IT to violate copyright, patent, trademark, or other intellectual property rights. Examples of violations include copying, distributing, altering, or translating copyrighted materials, software, music, or other media. To do any of these things, you need the copyright holder's permission or as allowed by law. See the UNC Libraries Scholarly Communications documentation.
10. Using University IT for personal business, commercial or political activities, fundraising, or advertising on behalf of non-University entities. The only exceptions are the limited allowance in the University's Personal Use Policy and the Policy on Use of University Resources in Support of Entrepreneurial Activities.
11. Extending or sharing the University network with the public or other people beyond what has been set up by ITS Communication Technologies/Networking. Do not connect any network devices or systems (like switches, routers, wireless access points, VPNs, and firewalls) to the University Network without consulting ITS Communication Technologies (see the University's Data Network Standard for details).
12. Failing to maintain security controls on any personal computing equipment that connects to University IT or that uses University Data. (See the Information Security Controls Standard.)

III. IT Security and Monitoring

The University may review or log any use of University IT. University access to e-mail on the University Network is allowed under the University's Policy on the Privacy of Electronic Information.

Reviewing or checking of University IT use may occur in the following situations if authorized personnel consider it necessary:

1. For generally accepted, network-administration practices;
2. To prevent or investigate 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, may contact local or federal law enforcement authorities to investigate any matter.

Exceptions

None.

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 to get, store, manipulate, manage, move, control, display, switch, swap, send, or receive data or information. The term information technology includes computers, mobile devices including phones, peripherals, dedicated smart devices, software (installed or provided by a third-party), services including network and support services, and related resources.

Spamming: Electronic junk mail or the abuse of electronic messaging systems to widely send bulk messages to people who did not request them.

Related Requirements

External Regulations and Consequences

- Copyright Act
- Digital Millennium Copyright Act
- N.C. Gen. Stat. § 143-805

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

Failure to follow this policy may put University information assets at risk. Employees who don't comply may face disciplinary consequences, up to and including losing their job. Students who don't comply may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors and vendors who don't comply 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.

University Policies, Standards, and Procedures

- Data Network Standard
- Information Security Controls Standard
- Personal Use Policy
- Policy on the Privacy of Electronic Information
- Policy on Use of University Resources in Support of Entrepreneurial Activities
- EHRA Non-Faculty Policies
- SHRA Policies
- Faculty Handbook
- Graduate School Handbook
- University Catalog

Please go to the Safe Computing at UNC webpage for more detailed information on securing a personal computer or network device.

Contact Information

Primary Contacts

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

Related Articles

Related Articles (3)

Adams School of Dentistry: Choose Your Own Device Policy

The UNC-Chapel Hill Adams School of Dentistry has a legal and ethical responsibility to safeguard patient information. This responsibility includes ensuring that devices storing Protected Health Information ("PHI") or other Sensitive Information are properly encrypted and are serviced by an appropriate vendor. The purpose of this Policy is to ensure that all Computing Devices used by students will meet institutional security requirements.

Information Security Policy

This policy defines a framework for the Information Security Program. It gives direction for policies, standards, and procedures that relate to security. These documents tell us how to include information security in all the ways we work at the University of North Carolina at Chapel Hill.

Policy on Terms of Use for Administrative Systems

This policy describes the terms required for use of ConnectCarolina, InfoPorte, associated reporting tools, and other University business applications (“Administrative Systems”).