POL 08.00.05
Acceptable Use Policy (AUP)

Authority: Chancellor

History:

- First Issued: 2003
- Revised: September 18, 2009; August 14, 2017
- Last Revised: October 30, 2018

Related Policies

- Statewide Information Security Manual
- NC Department of Information Technology Acceptable Use Policy

Additional References

- NCGS 14-454 Accessing Computers
- NCGS 14-455 Damaging Computers / Networks
- NCGS 132 Public Records Law

Contact Information: Associate Vice Chancellor for Technology Resources and Chief Information Officer, 910.775.4355.

1. PURPOSE

1.1 The **Acceptable Use Policy (AUP)** of the University of North Carolina at Pembroke sets forth the standards by which a student, faculty, staff, and authorized guest (users) may use their assigned computer systems and peripheral accessories, computer accounts, email services, and the shared University of North Carolina Pembroke (UNCP) network. The use of UNCP's computer and network resources including all electronic communication systems and equipment (all collectively referred to as the "UNCP information technology infrastructure") is a revocable privilege. By using or accessing the UNCP information technology infrastructure, users agree to comply with this policy and other applicable UNCP and UNC policies, as well as all applicable federal, state, and local laws and regulations. Using and/or accessing the UNCP information technology infrastructure without proper authorization is strictly prohibited.

2. RESPONSIBILITIES

2.1 The UNCP information technology infrastructure is provided to support UNCP university business and its mission of teaching, research, and service. Any uses that jeopardize the integrity of the UNCP information technology infrastructure or University data, the privacy or safety of other users, or that are otherwise illegal are prohibited. Users are responsible for being aware of any changes to this policy.

2.2 General guidelines for acceptable use of the UNCP information technology infrastructure are based on the following principles:

2.2.1. Users shall behave responsibly with respect to the UNCP information technology infrastructure at all times.

2.2.2. Users shall respect the integrity and the security of the UNCP information technology infrastructure.

2.2.3. Users shall behave in a manner consistent with UNCP's mission and comply with all applicable laws, regulations, UNCP policies, and policies of The University of North Carolina (UNC).

2.2.4. Users shall be considerate of the needs of other users by making every reasonable effort not to impede the ability of others to use the UNCP information technology infrastructure and to show restraint in the consumption of shared resources.

2.2.5. Users shall respect University principles regarding freedom of thought, inquiry and expression.

2.2.6. Users shall respect the rights and property of others, including intellectual property rights.

2.3 Conduct which violates this policy includes, but is not limited to:

2.3.1. Accessing the files, computers or data of another user or department without permission or authorization.

2.3.2. Sharing of account credentials (username, password, token) with others.

2.3.3. Using the UNCP campus network to gain unauthorized access to any computer system.

2.3.4. Using any means to decipher or otherwise obtain restricted passwords or access control information.

2.3.5. Attempting to circumvent or subvert the UNCP system or network security measures.

2.3.6. Allowing external parties access to the UNCP information technology infrastructure or agreeing to such (as defined in some peer-to-peer software licenses) unless for official university business which requires authorized appropriate documentation and adherence to federal, state and local, laws, policies, and guidelines.

2.3.7. Installing server software or modifying system configuration on any university system without the expressed authorization of DoIT.

2.3.8. Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to university data.

2.3.9. Performing any act, intentionally or otherwise, that will interfere with the normal operation of computers, peripherals, or networks.

2.3.10. The use of the UNCP information technology infrastructure to harass or intimidate others or to create a hostile work or educational environment.

2.3.11. Initiating or purposely propagating SPAM, Phishing, or other malicious content.

2.3.12. Forging the identity of a user or computer system in an electronic communication (spoofing).

2.3.13. Using email or network resources to solicit the UNCP community for political or personal gain, including without limitation solicitation for the purpose of selling items.

2.3.14. Copyright law violations, including but not limited to, providing copyrighted or licensed material to others while maintaining copies for one's own use, unless there is a specific provision in the license which allows this, or using a copyrighted program on more than one machine at the same time, unless this is permitted by a specific license provision. Users shall not store or transmit files in violation of copyright law on the UNCP information technology infrastructure.

2.3.15. Using the computer access privileges of others.

2.3.16. The use of the UNCP information technology infrastructure to launch or support DDoS (Distributed Denial of Service Attacks).

2.3.17. Engaging in conduct that violates applicable university policy or state or federal law.

3. MONITORING THE UNCP INFORMATION TECHNOLOGY INFRASTRUCTURE

3.1 UNCP expressly reserves the right to impose any restraints or monitor the content of communications, data or other information on the UNCP information technology infrastructure for the following reasons:

3.1.1. When required to do so by applicable federal, state or local laws, including without limitation laws that prohibit publication of defamatory material, laws requiring the disclosure of public records upon request, and laws prohibiting the misuse of state property for private gain;

3.1.2. To maintain the security and integrity of the UNCP information technology infrastructure and University data; or

3.1.3. To ensure the availability of email and other services to the UNCP community.

3.2 The UNCP information technology infrastructure may, subject to this policy, be used for incidental personal purposes, provided such use does not interfere with normal university operations, burden the university with incremental costs, violate laws, policies, or regulations or interfere with the user's employment or other obligations to the university. However, the University reserves the right:

3.2.1. To investigate any alleged AUP or other UNCP or UNC policy infractions; or

3.2.2. To assist in any internal or law enforcement investigations seeking evidence regarding alleged violation of any federal, state or local law or regulation.

3.3 Users shall have no expectation of privacy with any information on the UNCP information technology infrastructure. To the extent allowed by law, UNCP reserves the right to make any communications, data or information regarding, transmitted through, or stored on any part of the UNCP information technology infrastructure available to law enforcement officials without a search warrant and without prior notice to any user.

3.4 Users should use extreme caution in communicating, transmitting, or storing sensitive information on the UNCP information technology infrastructure. Although UNCP will comply with all legal obligations regarding confidentiality of certain statutorily identified records, users should not assume that information or data transmitted or stored on the UNCP information technology infrastructure is confidential or protected from disclosure to designated UNCP and UNC employees or law enforcement. UNCP cannot guarantee the confidentiality or integrity of any user's continuing access to any information or data stored or transmitted on UNCP's information technology infrastructure because of the possibility, despite UNCP's best efforts, of unauthorized access by third parties (hackers), failure of equipment (system crashes), or some other event. Users are reminded that UNCP may be required to disclose any information transmitted or stored on the UNCP information technology infrastructure that is determined to be a public record and not otherwise exempt from disclosure under applicable law. While every effort is made to ensure confidentiality and integrity, users are still responsible for maintaining the confidentiality of their personal access and authentication information (passwords, etc.) and for transmitting information (email, files, etc.) to the proper address.

3.5 In the event that such monitoring or review is necessary or appropriate, the Division of Information Technology or the Chancellor's designee will be responsible for such monitoring and preliminary investigations. General Counsel will lead the investigation, enforcement and coordination with the federal, state and / or local law enforcement agencies.

4. RESPONDING TO SECURITY AND ABUSE INCIDENTS

4.1 All users have the responsibility to report any discovered unauthorized access attempts or other improper usage of the UNCP information technology infrastructure or University data to the Division of Information Technology.

5. RANGE OF DISCIPLINARY ACTION

5.1 Persons in violation of this policy are subject to disciplinary action, including, but not limited to, the loss of computer or network access privileges, disciplinary action, and dismissal from UNCP. Any disciplinary actions against such individuals will be imposed through procedures consistent with any applicable UNC-GA, UNCP, federal, state and local regulations. Some violations may constitute criminal or civil offenses, as defined by local, state and federal laws, and the university may prosecute any such violations to the full extent of the law.

5.2 UNCP may suspend computer or network access privileges immediately and without prior notice to a user if necessary to preserve the safety or integrity of the UNCP information technology infrastructure and/or data, or to prevent or investigate violations of applicable federal, state or local law or UNCP or UNC policy. In the event that this policy conflicts with other UNCP or UNC policies, or federal or state legislation, the most restrictive policy or legislation shall apply.