

University Student and Employee Computer Use Regulation

Updated: December 16, 2016

POLICY:	REG08.05.04
TITLE:	University Student and Employee Computer Use Regulation
CATEGORY:	Information Technology
SUB-CATEGORY:	Security and Compliance
AUTHORITY:	Originally approved by Board of Trustees; Regulation updated by Chancellor
CONTACT:	Chief Information Officer (252) 328-9015
RELATED POLICIES:	Academic Computer Use University Record Retention Schedule University Student Code of Conduct
ADDITIONAL REFERENCES:	POL05.25.02 Notice of Nondiscrimination Policy NC General Statute 14-190-1, Obscene Literature & Exhibitions NC General Statute 14-456, Denial of Computer Services to an Authorized User NC General Statute 143B-920, Department Heads to Report Possible Violations of Criminal Statutes Involving Misuse of State Property to the State Bureau of Investigation U.S. Code Title 18, Section 1030, Fraud and Related Activity in Connection with Computers North Carolina State Personnel Manual North Carolina Division of State Archives EDUCAUSE
HISTORY:	Policy Number 1.500 Supersedes Policy Dated: June 30, 1999 Effective Date: September 25, 2003 Review Date: September 26, 2011 Placed in University Policy Manual after EXPEDITED REVIEW, transitioned without substantive change from prior version, March 25, 2013; Revised December 16, 2016
PREVIOUS VERSIONS:	No previous versions available.

1. Introduction

1.1. Purpose of Regulation.

1.1.1. To govern the use of East Carolina University ("University") computer systems, which includes hardware, data, software and communications networks.

1.2. Person(s) with Primary Responsibility.

1.2.1. Chief Information Officer.

2. Regulation Outline

2.1. This regulation applies to all University students and employees whether full time, part time, temporary, or volunteer, but excludes faculty who are governed by the Academic Computer Use Policy.

2.2. Freedom of expression is limited to no greater degree in electronic format than in printed or oral communication. Individual employees or students are entitled to full freedom in research and the publication of those results to include freedom of speech and freedom of artistic expression through electronic means as well as in familiar and traditional media. Electronic means of freedom includes the respect for open forum communications free of harassment and discrimination. Intellectual property in electronic form is as fully protected as are those properties in other forms. It is important for all users to behave in a responsible, ethical and legal manner. In general, appropriate use means respecting the rights of other computer users, the integrity of the physical facilities and all pertinent license and contractual agreements.

2.3. The University provides academic access to a functioning system of electronic communication on a nondiscriminatory basis, without regard to the perceived merit of a particular content or subject matter or the views of users. The University is committed to equality of opportunity and prohibits unlawful denial of access based on the following protected classes: race/ethnicity, color, genetic

information, national origin, religion, sex (including pregnancy and pregnancy related conditions), sexual orientation, gender identity, age, disability, political affiliation, or veteran status.

2.4. This regulation applies to all University procured and managed computer systems including hardware, data, software, and the communication networks associated with these systems. In addition, this regulation applies to all non-university owned computers connected to the University's network and to all users of computing resources owned or managed by the University, including, but not limited to, University employees, students, guests, external individuals or organizations and individuals accessing University computing resources through external network services, such as the Internet.

2.5. Individual employees and students shall make every effort to show that they are not speaking for the University when they are not officially authorized to do so. Unless officially authorized by the University, individual users must avoid or dispel any inference that their views represent the views of the University. Individual employees and students are responsible for following applicable federal and state laws, and the University of North Carolina Board of Governors ("UNC"), and University policies, regulations and rules.

3. Regulatory Limitations

3.1. The University reserves the right to limit employee and student computing resource access when federal or state laws or University policies, regulations and rules are violated or when University contractual obligations or University operations may be impeded.

3.2. The University may authorize confidential passwords or other secure entry identification; however, employees and students have no expectation of privacy in the material sent or received by them over University computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified in this regulation.

3.3. The University has the right to monitor network traffic, including electronic mail (e-mail), to and from privately owned machines connected to the University network within the limitations of this regulation. The University generally does not monitor or restrict material residing on University computers housed within a private domicile or on non-University computers, whether or not such computers are attached or able to connect to campus networks. However, if University Administration is informed of inappropriate employee or student conduct associated with computing resource use, it is obligated to investigate and enforce applicable federal and state laws, and the policies, regulations and rules of UNC and the University.

3.4. All material prepared and utilized for work purposes and posted to or sent over University computing and other telecommunication equipment, systems or networks must be accurate and must correctly identify the creator of such.

3.5. The University may monitor access to its equipment and networking structures and systems to insure the security and operating performance of its systems and networks and to enforce or comply with UNC or University policies, regulations and rules. Monitoring or otherwise accessing of individual employee and student computers to enforce UNC or University policies, regulations or rules requires specific approval of the Chancellor.

4. Permissible Uses

4.1. Employees and students are expected to follow this regulation and any UNC or University policies, regulations and rules applicable to University work produced on computing equipment, systems and networks. Employees and students may access these technologies for personal use, subject to the following restrictions:

4.1.1. The use is lawful under federal and state law.

4.1.2. The use is not prohibited by UNC or University policies, regulations or rules.

4.1.3. The use does not overload University computer equipment or systems, or otherwise harm or negatively impact the system's performance.

4.1.4. The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies).

4.1.5. The use does not violate federal or state laws or UNC or University policies, regulations or rules on copyright and trademark.

4.1.6. The use does not state or imply University sponsorship or endorsement.

4.1.7. The use does not violate federal or state laws or UNC or University policies, regulations or rules against illegal discrimination, including sexual harassment.

4.1.8. The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security or in any way attempts to gain unauthorized access.

4.1.9. The use, when performed for non-work related activity, does not conflict with regular work assignments and does not represent more than incidental use for non-faculty employees.

4.1.10. The use does not conflict the rights and privacy of others or violate any UNC or University policy, regulation or rule, or any state or federal law. Access to computing resources is a privilege that is granted on the presumption that every member of the University community will act responsibly. The University endorses the following statement on software and intellectual rights distributed by EDUCAUSE, the non-profit consortium of colleges and universities committed to the use and management of information technology in higher education and the Information Technology Association of America (ITAA), a leading industry trade group for information technology companies:

“Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to work of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy and right to determine the form, manner and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.”

5. Other Computer Use Guidelines

5.1. Users are to have valid authorized accounts and may only use those computer resources, which are specifically authorized. Users are responsible for taking reasonable precautions to safeguard their own computer account. Users should treat computing resources and electronic information as a valuable University resource.

5.2. Users who publish home pages on the Internet must identify themselves as the author. In addition, they must include the disclaimer that follows, or a similar disclaimer stating that any personal home page content reflects their own views and not necessarily those of the University. This disclaimer must appear on the main page and any subsequent page where the users' (author's) name appears on the user's web site. East Carolina University is not responsible for either the contents of this web page or any other page that can be linked from this web page and that the material is not endorsed, sponsored or provided by or on behalf of the University. In addition, any links to other web resources must be clearly identified.

5.3. Users may not change copy, delete, read or otherwise access files or software owned by other parties without permission of the custodian of the files or the system administrator. Users may not bypass accounting or security mechanisms to circumvent data protection measures. Users may not attempt to modify software except when intended to be user customized. Users shall assume that any software they did not create is copyrighted. They may neither distribute copyrighted proprietary material without the written consent of the copyright holder nor violate copyright or patent laws concerning computer software, documentation or other tangible assets.

5.4. Employees must not use the computer systems to violate any rules in the East Carolina University Business Manual, North Carolina State Personnel Manual, departmental rules, UNC or University policies, regulations or rules, or any local, state or federal laws.

5.5. Students must not use the computer systems to violate any rules in the East Carolina University Student Code of Conduct, departmental rules, or any local, state or federal laws.

6. State and Federal Statutes

6.1. North Carolina statutes of which individual employees and students should be aware of that may bear on computer use include:

6.1.1. North Carolina General Statute 14-190-1, Obscene Literature and Exhibitions;

6.1.2. North Carolina General Statute 144-456, Denial of Computer Services to an Authorized User; and

6.1.3. North Carolina General Statute 143B-920, Department Heads to Report Possible Violations of Criminal Statutes Involving Misuse of State Property to the State Bureau of Investigation.

6.2. Federal statutes of which individual employees and students should be aware of that may bear on computer use include:

6.2.1. U.S. Code Title 18, Section 1030, Fraud and Related Activity in Connection with Computers.

7. Violation of Regulation by University Employees

7.1. Any violation of this regulation is “misconduct” under EHRA policies (EHRA non-faculty) and “unacceptable personal conduct” under SHRA policies. Sanctions for violation of this regulation may include one or more of the following:

7.1.1. A revocation of access privileges;

7.1.2. A written warning or written reprimand; demotion; suspension without pay; or

7.1.3. Dismissal.

7.2. Violations of law may also be referred for criminal or civil prosecution.

7.3. Violations of this regulation should be reported immediately to:

7.3.1. The employee's unit administrator;

7.3.2. Upon verification reported by the unit administrator to Employee Relations in the Department of Human Resources; and

7.3.3. In consideration of violation severity, Employee Relations will notify the Office of University Counsel and the Chief Information Officer. (Upon notification, the Chief Information Officer may terminate computing resource access privileges pending investigation of the violation).

8. Application of Public Records Act

8.1. All information created or received for work purposes and contained in University computing equipment files, servers or electronic mail (e-mail) depositories are public records and are available to the public unless an exception to the Public Records Act

applies. This information may be purged or destroyed only in accordance with the University records retention schedule and State Division of Archives regulations.

9. Violation of Regulation by Students

9.1. Any violation of this regulation is “misconduct” under the University’s student conduct code. Violations should be reported as provided in that code. Sanctions for violation of this regulation may include revocation or suspension of access privileges in addition to any other sanction permitted under the student conduct code. Violations of law may also be referred for criminal or civil prosecution.

10. Regulation Questions

10.1. Employees’ questions or concerns about this regulation should be directed to the office of Human Resources. Students’ questions or concerns about this regulation should be directed to the office of the Dean of Students, Student Life.