



April 7, 1998

Office of the Chancellor
103 Spilman

919-328-6212

Professor Don Sexauer
Chair of the Faculty
140 Rawl Annex
East Carolina University

Re: Academic Computer Use Policy

Dear Professor Sexauer:

I am pleased to approve Faculty Senate Resolutions 98-9, 98-11, and 98-12 as submitted. As I reported to the Faculty Senate, I cannot approve Resolution 98-10 in the recommended form.

My concern with Resolution 98-10, University Academic Computer Use Policy, centers on my understanding of the Public Records Act of North Carolina. My reading of that law and recent court decisions related thereto lead me to the inescapable conclusion that state-owned computer systems and records, including e-mail, are subject to inspection under law. Thus, proposed language that appears to assure confidentiality and privacy is misleading and potentially harmful to individual computer users. Therefore, I am approving a University Academic Computer Use Policy that is based upon the Faculty Senate Resolution 98-10, but includes deletions and additions. Specifically, I have decided to delete paragraphs 6, 7 and 8 of the policy submitted to me by the Senate and to substitute the following paragraphs:

Regulatory Limitations

The University may monitor access to the equipment and networking structures and systems to insure the security and operating performance of its systems and networks and to enforce University policies. Monitoring or otherwise accessing individual faculty member's computers to enforce University policies requires specific approval of the Chancellor.

Professor DonSexauer

Page 2

April 7, 1998

The University reserves the right to limit access when federal or state laws or University policies are violated or where University contractual obligations or University operations may be impeded.

The University may authorize confidential passwords or other secure entry identification; however, employees have no expectation of privacy in the material sent or received by them over the University computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified above. Again, monitoring or otherwise accessing individual faculty member's computers to enforce University policies requires specific approval of the Chancellor.

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.

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 and receiver of such.

I have also decided to add a section entitled "Permissible Uses" which will appear in the approved policy directly after the section entitled "Regulatory Limitations" which is quoted directly above. The text of this additional section is as follows:

Permissible Uses

Faculty members are expected to follow this policy and any related University rules, regulations and procedures for University work produced on computing equipment, systems and networks. Faculty members may access these technologies for personal uses if the following restrictions are followed:

- (1) The use is lawful under federal or state law.
- (2) The use is not prohibited by Board of Governors, University or institutional policies.

Professor Don Sexauer

Page 3

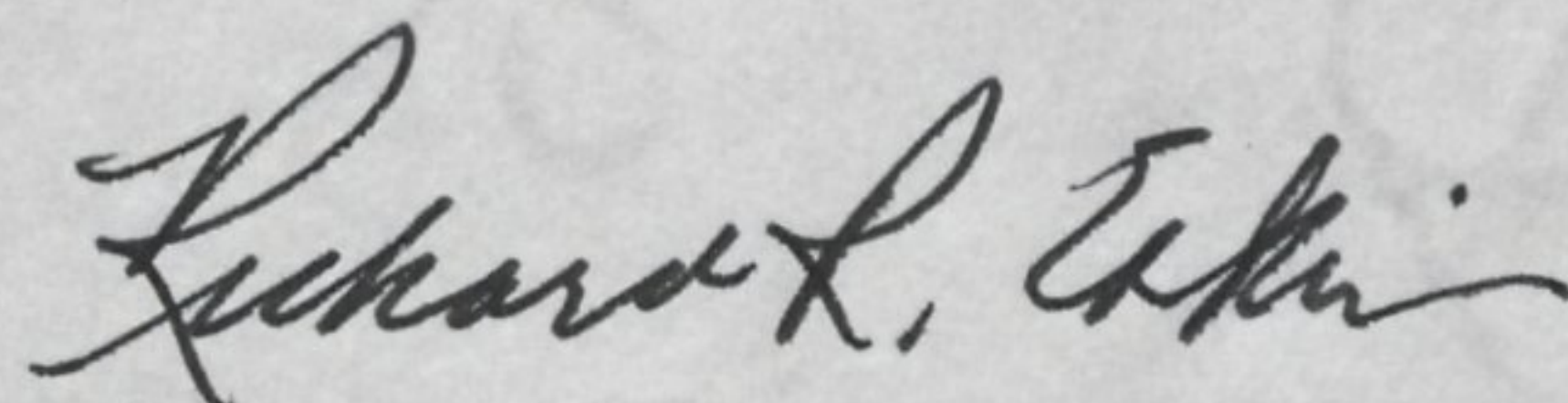
April 7, 1998

- (3) The use does not overload the University computer equipment or systems, or otherwise harm or negatively impact the system's performance.
- (4) The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies).
- (5) The use does not violate federal or state laws or University policies on copyright and trademark.
- (6) The use does not state or imply University sponsorship or endorsement.
- (7) The use does not violate state or federal laws or University policies against race or sex discrimination, including sexual harassment.
- (8) The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security in any way attempts to gain unauthorized access.

I am enclosing a copy of the Academic Computer Use Policy which illustrates the additions and deletions. I am also enclosing a clean copy of the Policy as I have approved it.

Please know that I have taken this step to amend the resolution of the Faculty Senate only after all reasonable attempts to reach a compromise version of the policy have been exhausted. I would have preferred a consensus policy statement but that did not seem possible despite our common best efforts.

Sincerely,



Richard R. Eakin

RRE:pnb
Enclosures

ACADEMIC COMPUTER USE POLICY

Freedom of expression and academic freedom are limited to no greater degree in electronic formats than in printed or oral communication. Individual faculty members are entitled to full freedom in research and in the publication of results. Academic freedom includes freedom of artistic expression through electronic means as well as in familiar and traditional media. Intellectual property in electronic form is as fully protected as are those properties in other forms. Individual faculty members are entitled to freedom in the classroom in discussing their subject, including those formats used in virtual spaces and areas where communication is inherent in the teaching and learning process.

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. Equality of access is assured without regard to race, gender, nationality, age, religion, disability, or sexual orientation.

The University relies heavily upon its computer information systems to meet operational, financial, educational and informational needs. It is essential that East Carolina University's computer systems, and computer networks, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner. It is critical that these systems and machines be protected from misuse and unauthorized access.

This policy applies to University computer systems and refers to hardware, data, software and communications networks associated with these computers. In particular, this policy covers computers ranging from multi-user timesharing systems to single user personal computers, whether stand-alone or connected to the network.

Individual faculty members shall make every effort to show that they are not speaking for the University when they are not. Special care shall be taken in posting or distributing digital material, on a web page or site created and accessed through the University computing system. Individual faculty members must avoid or dispel any inference that the speaker represents the views of the University or of faculty colleagues. Individual faculty members are responsible for following federal, state, University of North Carolina Board of Governors, and University laws and policies.

~~The University shall respect the privacy and confidentiality of Internet use by individual faculty members as the University respects the use of University libraries by individual faculty members. Personal, professional, and research files and communications are normally excluded except in following cases. Administrative documentation of all research projects requiring University authorization are deemed "public records" under the State Public Records Act and are subject to that act's retention and disposition requirements. Official copies of grant applications, required reports, financial, personnel, and other administrative materials are handled by and retained with the University. All records in electronic formats concerning, or generated in the course of conducting University programs, projects, administration, representation, or other business, are "public records" as defined by the state records act and, so, subject to that act's retention/disposition requirements in the same manner as paper records.~~

~~The University shall respect the privacy and confidentiality of E-mail communications and other faculty documents that are not public documents as defined by North Carolina Statute 132. With few exceptions (e.g., convenience copies of student grades), papers of individual faculty members are considered the property of the faculty member and not of the University. Those records that are created by a faculty member serving as an administrator (i.e., department chair, chair of a faculty committee, principal investigator of a University-authorized research project) are the official records of that office or activity. They are deemed "public records" under the state records act and, so, are subject to that act's retention and disposition as well as maintenance requirements. Otherwise, E-mail and other faculty documents shall not be examined by the University unless authorized by the chancellor, or by permission of the individual faculty member. Any faculty member whose documents, files, or other computer data is examined shall be notified within 10 days. The notification shall provide a description of what was examined and the reasons for such an examination.~~

~~The respect of the University for the privacy and confidentiality of the foregoing is an essential part of academic freedom.~~

Regulatory Limitations

The University may monitor access to the equipment and networking structures and systems to insure the security and operating performance of its systems and networks and to enforce University policies. Monitoring or otherwise accessing individual faculty member's computers to enforce University policies requires specific approval of the Chancellor.

The University reserves the right to limit access when federal or state laws or University policies are violated or where University contractual obligations or University operations may be impeded.

The University may authorize confidential passwords or other secure entry identification; however, employees have no expectation of privacy in the material sent or received by them over the University computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified above. Again, monitoring or otherwise accessing individual faculty member's computers to enforce University policies requires specific approval of the Chancellor.

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.

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 and receiver of such.

Permissible Uses

Faculty members are expected to follow this policy and any related University rules, regulations and procedures for University work produced on computing equipment, systems and networks. Faculty members may access these technologies for personal uses if the following restrictions are followed:

- (1) The use is lawful under federal or state law.
- (2) The use is not prohibited by Board of Governors, University or institutional policies.

- (3) The use does not overload the University computer equipment or systems, or otherwise harm or negatively impact the system's performance.
- (4) The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies).
- (5) The use does not violate federal or state laws or University policies on copyright and trademark.
- (6) The use does not state or imply University sponsorship or endorsement.
- (7) The use does not violate state or federal laws or University policies against race or sex discrimination, including sexual harassment.
- (8) The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security in any way attempts to gain unauthorized access.

Other Computer Usage Guidelines

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 who choose to publish home pages on the World Wide Web must identify themselves as the author. In addition, they must include a disclaimer that any personal home page content reflects their own views and not necessarily that of the University. Furthermore, any links to other web resources must be identified.

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 schemes. 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.

Users must not use the computer systems to violate any rules in the East Carolina University Faculty Manual, or any local, state or federal laws.

University policies stated in the Faculty Manual of which individual faculty members should be aware that may bear on computer use include Part IV, Section V, External Professional Activities for Pay; Part VII, Section II.G., Copyright Procedures; Appendix I, East Carolina University Policy on Conflicts of Interest and Commitment.

North Carolina statutes of which individual faculty members should be aware that may bear on computer use include 14-190-1, Obscene Literature and Exhibitions; 114-15.1. Denial of Computer Services to an Authorized User; 114-14.1 Department Heads to Report Possible Violations of Criminal Statutes Involving Misuse of State Property to the State Bureau of Investigation. United States statutes of which individual faculty members should be aware that indirectly may bear on computer use include Title 18, Section 1030, Fraud and Related Activity in Connection with Computers.”

ACADEMIC COMPUTER USE POLICY

Freedom of expression and academic freedom are limited to no greater degree in electronic formats than in printed or oral communication. Individual faculty members are entitled to full freedom in research and in the publication of results. Academic freedom includes freedom of artistic expression through electronic means as well as in familiar and traditional media. Intellectual property in electronic form is as fully protected as are those properties in other forms. Individual faculty members are entitled to freedom in the classroom in discussing their subject, including those formats used in virtual spaces and areas where communication is inherent in the teaching and learning process.

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. Equality of access is assured without regard to race, gender, nationality, age, religion, disability, or sexual orientation.

The University relies heavily upon its computer information systems to meet operational, financial, educational and informational needs. It is essential that East Carolina University's computer systems, and computer networks, as well as the data they store and process, be operated and maintained in a secure environment and in a responsible manner. It is critical that these systems and machines be protected from misuse and unauthorized access.

This policy applies to University computer systems and refers to hardware, data, software and communications networks associated with these computers. In particular, this policy covers computers ranging from multi-user timesharing systems to single user personal computers, whether stand-alone or connected to the network.

Individual faculty members shall make every effort to show that they are not speaking for the University when they are not. Special care shall be taken in posting or distributing digital material, on a web page or site created and accessed through the University computing system. Individual faculty members must avoid or dispel any inference that the speaker represents the views of the University or of faculty colleagues. Individual faculty members are responsible for following federal, state, University of North Carolina Board of Governors, and University laws and policies.

Regulatory Limitations

The University may monitor access to the equipment and networking structures and systems to insure the security and operating performance of its systems and networks and to enforce University policies. Monitoring or otherwise accessing individual faculty member's computers to enforce University policies requires specific approval of the Chancellor.

The University reserves the right to limit access when federal or state laws or University policies are violated or where University contractual obligations or University operations may be impeded.

The University may authorize confidential passwords or other secure entry identification; however, employees have no expectation of privacy in the material sent or received by them over the University computing systems or networks. While general content review will not be undertaken, monitoring of this material may occur for the reasons specified above. Again, monitoring or otherwise accessing individual faculty member's computers to enforce University policies requires specific approval of the Chancellor.

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.

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 and receiver of such.

Permissible Uses

Faculty members are expected to follow this policy and any related University rules, regulations and procedures for University work produced on computing equipment, systems and networks. Faculty members may access these technologies for personal uses if the following restrictions are followed:

1. The use is lawful under federal or state law.

2. The use is not prohibited by Board of Governors, University or institutional policies.
3. The use does not overload the University computer equipment or systems, or otherwise harm or negatively impact the system's performance.
4. The use does not result in commercial gain or private profit (other than allowable under University intellectual property policies.)
5. The use does not violate federal or state laws or University policies on copyright and trademark.
6. The use does not state or imply University sponsorship or endorsement.
7. The use does not violate state or federal laws or University policies against race or sex discrimination, including sexual harassment.
8. The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security in any way attempts to gain unauthorized access.

Other Computer Usage Guidelines

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 who choose to publish home pages on the World Wide Web must identify themselves as the author. In addition, they must include a disclaimer that any personal home page content reflects their own views and not necessarily that of the University. Furthermore, any links to other web resources must be identified.

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 schemes. 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.

Users must not use the computer systems to violate any rules in the East Carolina University Faculty Manual, or any local, state or federal laws.

University policies stated in the Faculty Manual of which individual faculty members should be aware that may bear on computer use include Part IV, Section V, External Professional Activities for Pay; Part VII, Section II.G., Copyright Procedures; Appendix I, East Carolina University Policy on Conflicts of Interest and Commitment.

North Carolina statutes of which individual faculty members should be aware that may bear on computer use include 14-190-1, Obscene Literature and Exhibitions; 114-15.1. Denial of Computer Services to an Authorized User; 114-14.1 Department Heads to Report Possible Violations of Criminal Statutes Involving Misuse of State Property to the State Bureau of Investigation. United States statutes of which individual faculty members should be aware that indirectly may bear on computer use include Title 18, Section 1030, Fraud and Related Activity in Connection with Computers.”