3-18 Policy for Responsible Use of Technological Resources

Purpose

In support of the college's mission to provide accessible education and training, College of The Albemarle provides access to computing and information resources for students, faculty, staff, and other authorized individuals.

The Policy for Responsible Use of Technological Resources at College of The Albemarle reflects the governing philosophy for regulating faculty, staff, student, and other authorized individuals use of the college's computing resources. It spells out the general principles regarding appropriate use of equipment, software, and networks. By adopting this policy, the college recognizes that all members of the college are also bound by federal, state, and local laws relating to copyrights, security, and other statutes regarding electronic media. The policy also recognizes the responsibility of faculty, staff and students for seeing that the computing resources are used in an effective, efficient, ethical, and lawful manner. Furthermore, the policy also recognizes the responsibility of faculty and system administrators taking a leadership role in implementing the policy and assuring that the college community honors the policy.

Definitions of Terms

Administrative Officer: Vice President, Dean, Chair, or Director to whom an individual reports.

Computer account: The combination of a user number, user name, or user I.D., and a password that allows an individual access to a mainframe computer or some other shared computer or network.

Information Resources: Data or information as well as the software and/or hardware that make the data or information available to users.

Network: A group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.

Privacy: No right of privacy exists in the use of technological resources. Much of the information created, transmitted or stored on college technological resources are subject to the North Carolina Public Records Act. Users should not assume that files or communications created, transmitted or stored using college resources will be private. College administrators or individuals designated by the

President may review any files, monitor all communications and intercept e-mail or other messages to maintain system integrity and ensure compliance with college policies and applicable laws and regulations.

Servers: **"**Central" computers capable of use by several people at once.

Software: Programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, or optical (CDs, DVDs), etc.). Usually used to refer to computer programs.

System Administrator: Staff employed by a central computing agency such as Management Information Services whose responsibilities include system, site, or network administration and staff employed by other college departments whose duties include system, site, or network administration.

System administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. If a person has a computer on his/her desk, he/she may be acting, in whole or in part, as that system's system administrator.

User: Anyone who does not have system administrator responsibilities for a computer system or network but who makes use of that computer system or network. A user is responsible for his/her use of the computer and for learning proper data management strategies.

I. Policy for Responsible Administrative ~~Computing~~ Use of Technological Resources

The following rules and prohibitions define acceptable use of the college technological resources whose primary users are faculty and staff using the system for college business (i.e. the technological resources in the Management Information Services Department). Unacceptable use is prohibited and is grounds for loss of technological resource privileges, as well as disciplinary or legal sanctions under federal, state, or local law.

All users of this system must comply with the principles outlined in this policy. By using this system, users agree that they understand and will comply with these principles:

1. The college owns the system. All information contained on the system is college property. The college reserves all rights to the system, including termination of service without notice. Users of this system have rights that

may be protected by federal, state, and local law. Statements required by some acts of law can be found in this document under the section headed: **Disclaimers.**

2. Computer facilities and accounts are owned by the college and are to be used for college-related activities only. Acceptable uses are limited to responsible, efficient and legal activities that support learning and teaching. College technological resources are not to be used for commercial purposes or non-college related activities without written authorization from the college. Written authorization must come through the Technology Committee and then through the President's office for final approval. All access to central computer systems, including the issuance of passwords, must be approved through the office of Management Information Services (MIS).

3. The use of college technological resources, including access to the internet and college network, is a privilege, not right. Responsible use of college technological resources is use that is ethical, respectful, academically honest and consistent with the college's mission. Users are expected to abide by the generally accepted rules of network etiquette.

4. A computer account assigned to an individual by MIS must not be used by others without explicit permission from the administrative officer who requested the account. The individual is responsible for the proper use of the account, including proper password protection. Do not share computer accounts. If someone else learns a person's password, that individual must change it. Report unauthorized use of accounts to the Project Director, Supervisor, System Administrator or other appropriate college administrative officer.

5. Programs and files are confidential unless they have explicitly been made available to other authorized individuals. The college reserves the right to access all information stored on college computers. When performing maintenance, reasonable efforts will be made to ensure the integrity of a user's files. However, if violations are discovered, they will be reported immediately to the appropriate administrative officer.

6. Electronic communications facilities (such as MAIL) are for college-related activities only. The college supports the State's policy on the use of college owned and the state operated network. All users will conform to the

acceptable use policies for the North Carolina Integrated Information Network (NCIIN).

7. Users must respect the privacy of others and may not reveal personally identifying information, or information that is private or confidential, such as confidential student or personnel information, home addresses and phone numbers, credit or checking account information, or social security numbers.

8. Sending fraudulent computer mail, breaking into another user's electronic mailbox, or reading someone else's electronic mail without his or her permission are some, but not all, actions that can be characterized as misuse of the computing resources.

9. Harassing, threatening, or obscene messages and/or materials are not to be created, sent, received, displayed, or stored.

10. No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any college computer system.

11. The college provides virus scanning software that is used on all computers within the college. Users that bring data to the college computers must scan the media before using it on any computer. The college supported anti-virus software must not be disabled or tampered with by the end users.

12. Computer software protected by copyright is not to be copied from, into, or by using campus computing facilities except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied to make backup copies, if permitted by the copyright owner. The number of copies and distribution may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

13. Users are not authorized to install new software, or updates to existing software on the college-owned computers. All desktop and laptop computers are configured in standard formats for administrative and instructional users. These configurations are developed and tested by the Management Information Services Department. If a user needs additional software installed on their office computer or in a computer classroom, they should submit a work request to Management Information Services for this

purpose. Exceptions to this policy must be approved by the Director of Management Information Services. Users should not install copies of personally owned software on college desktop computers or laptops. Unauthorized software found on college computers will be removed by the PC Support Technician.

14. All departments that own technological equipment are encouraged to develop "Conditions of Use" or "Guidelines for Responsible Use of Technological Resources" documentation for all systems that they operate and to make these documents available to users. These documents should be consistent with the college's Policy on Responsible Use of Technological Resources and should be approved by the department's administrative officer or other individual designated by that administrative officer. A copy of the "Conditions of Use" or "Guidelines for Responsible Use of Technological Resources" documentation should be sent to the Director of Management Information Services.

15. Users are not authorized to directly connect personally owned computers or laptops to the college internal network. Users can access the college's internet via the wireless network, however, please be advised that the wireless network is not encrypted. Use at your own risk. We do encourage users to make sure their anti-virus and operating system is up to date before accessing the wireless network. College of The Albemarle is not responsible for any tech support for any personal computers. The college does have the right to deny access from the wireless network.

    The college uses several methods to protect the computer systems and critical information within the wide-area network operated by the college. A firewall server protects the internal network by limiting access from external sources to only the servers intended for public access, the college web server and the online courses server. The internal network has been further subdivided into VLAN's (Virtual Local Area Networks) that isolate traffic by port and end user. The college installs anti-virus software on all desktop and laptop computers along with client/server software. The client/server software provides a method of regularly updating the anti-virus definitions.

    If an unauthorized computer or laptop is connected to the internal network, there is a possibility that a program or virus will be introduced that will disrupt the function of the network and/or the authorized computers connected to the network. Users that violate this policy may be held accountable for the expenses caused by such a disruption.

II. Policy for Responsible Instructional ~~Computing~~ Use of Technological Resources

The following rules and prohibitions define acceptable use of all college technological resources whose primary users are faculty, staff, students, and other authorized individuals. The instructional technological resources are to be used to support the educational programs of the college and are to be used for such related activities only. College technological resources are not to be used for commercial purposes or non-college related activities. Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as, prosecution under federal, state, and local law.

All users of the college's instructional technological resources must comply with the policies outlined in this document. By using any of these systems, users agree that they will comply with these policies.

1. The college reserves all rights, including termination of services without notice, to the instructional technological resources that it owns and operates. Users of these systems have rights that may need to be protected by federal, state and local law. Statements required by some acts of law can be found in this document under the section headed: **Disclaimers.**

2. Access and privileges to the college instructional technological resources are assigned and managed by the system administrators of specific individual systems. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system. Users may not, under any circumstances, transfer or confer these privileges to other individuals. Any account assigned to an individual shall not be used by others without written permission from the system administrator. The authorized user is responsible for the proper use of the system, including password protection.

3. USER RESPONSIBILITIES:

    a. Maintain an environment in which resources are shared equitably between users:

        - The system administrator of each system sets minimum guidelines within which users must conduct their activities.

    b. Maintain an environment that is conducive to learning:

- A user who harasses or makes defamatory remarks, is subject to disciplinary action up to and including dismissal from the college. Further, by using the system, users agree that individuals who transmit such remarks shall bear sole responsibility for his/her actions. Users agree that the college's role in managing this system is only as an information carrier, and that he/she will never consider transmission through this system as an endorsement of said transmission by the college.

- Many of the college's instructional technological resources provide access to outside networks both public and private which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that the college does not assume responsibility for the contents of any of these outside networks. The user agrees to comply with the acceptable use guidelines for any outside networks or services he/she may access through the college systems. Further, the user agrees to follow proper etiquette on outside networks as defined by that network.

- The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading. The user agrees never to attempt to transmit, or cause to be transmitted, any message that is inconsistent with an environment conducive to learning or with a misleading origination. The person who performed the transmission will be solely accountable for the message, not the college, which is acting solely as the information carrier.

- The user shall not use the system in such a manner as to disrupt the business of the college by creating, displaying, transmitting, receiving or making accessible threatening, racist, sexist, obscene, offensive, annoying or harassing language and/or material, including broadcasting unsolicited messages or sending unwanted mail or otherwise.

c. Maintain an environment free of illegal or malicious acts:

- The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which he/she is authorized, or any attempt to deprive other authorized users

of information resources or access to any college computer system shall be regarded as malicious, and may be treated as an illegal act.

d. Maintain a secure environment:

- Knowledge of passwords or loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of technological resources for which proper authorization has not been given.

- Users are responsible for proper password maintenance, including periodic changes and safeguarding the password.

- Users are responsible for backup of their own data.

4. Computer software protected by copyright shall not be copied from, into, or by means of college technological resource facilities, except as permitted by law or by the contract with the owner of the copyright. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users exceeds the number of original copies purchased.

5. PRIVATE MACHINES CONNECTED TO THE COLLEGE NETWORK:

   Computers that are not college owned are not authorized to directly connect to the college network. Users can access the colleges Internet via the wireless network, however, please be advised that the wireless network is not encrypted. Use at our own risk. College of The Albemarle is not responsible for any tech support for any personal computers. We do encourage users to make sure their anti-virus and operating system is up to date before accessing the wireless network. The college does have the right to deny access from the wireless network if needed.

   Computer systems owned by students, faculty, or staff that are using the college's wireless network are subject to all policies stated in this document.

   a. A private machine connected to the college network may not be used to provide network access to individuals who would not have access through official college systems. The private machine may not be used as a router to other networks nor may it serve in any way as an electronic gateway to non-college affiliated systems.

b. Private machines may not use the college network for commercial gain or profit.

c. Private machines may be used to support anonymous ftp, http, or gopher services when these services fall within the definition of scholarly use. Provision of interactive login services to non-college affiliated users is forbidden.

d. Should the college have reason to believe that a privately owned system is using the network inappropriately, network traffic to and from that system will be monitored and, if justified, the system will be disconnected and action taken with appropriate authorities.

Unless otherwise expressly modified by this Section II, the requirements and restrictions of Section I of this policy apply to Instructional Use of Technological Resources.

III Responsibilities of System Administrators

System administrators' use of the colleges' technological resources is governed by the same guidelines as any other user's technological resource activity.

However, system administrators have additional responsibilities to the network, site, and system(s) he/she administers.

1. System administrators will respect user's privacy, and will not examine mail except in the following circumstances:

   - Investigating an apparent violation of these policies, any other college policy, any law or regulation;
   - Disk capacities are exceeded and the user's mail storage is a contributing factor;
   - Performing routine monitoring of the system to ensure compliance with this policy, other College policies and applicable laws and regulations;
   - Performing any necessary maintenance of the system;
   - Forwarding missed-delivered messages; or
   - Closing an account that contains unread mail.

2. System administrators are responsible for the security of a system, network or server.

3. System administrators must take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on all systems, networks, and servers for which he/she has responsibility.

4. System administrators must take reasonable precautions to guard against corruption of data or software or damage to hardware or facilities.

5. System administrators must respect the proper usage of the system and will not share information gathered from any monitoring or inspection except as necessary from the performance of their duties.

6. System administrators may develop additional more detailed guidelines, as needed, for any of the college technological resources. These guidelines will cover such issues as allowable connect time and disk space, handling of unretrievable mail, responsibility for account approval and other items related to administering the system. These documents must be consistent with the college's Policy for Responsible Use of Technological Resources and should be approved by the department's administrative officer or other individual designated by that administrative officer.

IV. Disclaimers

The following are statements regarding the college computer systems that are currently mandated, or may soon be mandated, by federal or state law or current college policy.

Electronic Mail Privacy – Two accounts on the college system have the ability to read individual mail: the individual's account and the system administrator account. While reasonable attempts will be made to ensure the privacy of electronic mail, there is no guarantee that electronic mail is private. The college system is not a secure system nor is it connected to a secure network. Discriminatory conduct will be addressed through the College's Civil Rights/Nondiscrimination Policy.

Conduct that is considered to be sexually harassing will be addressed through the College's Unlawful Harassment Policy and Procedure.

V. Violations of Policy

Any users' privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be confidentially reported to the appropriate college official(s). Violations of these policies will be dealt with in the same manner as violations of other college policies and may result in disciplinary action. The full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the college, and legal action. Violations of the procedures may constitute a criminal offense. Any user who files a complaint or otherwise protests against discrimination has the right to be free from any retaliatory action because of the complaint or protest. Any user who protests against discriminatory conduct and who is subsequently subject to retaliatory action because of the protests may file an additional or amended complaint with the appropriate college official.