A. General

1. College owned or operated computer resources are intended for the use of its faculty, students, staff and other authorized individuals for purposes directly related to instruction and administrative activities. Access to these resources is a privilege. Those granted privileges are responsible for using resources in an effective, ethical and lawful manner. The college does not attempt to articulate all required or unacceptable behavior by its users of the computer resources at Gaston College. This policy is in addition to and complements any existing or future policies relating to the use of computers and technology.

2. Each user is required to read and certify that he or she understands this policy relating to acceptable use of Gaston College computer resources.

B. Acceptable Use Policies

1. Access and privileges of College's information systems are assigned and managed by the Chief Technology Officer. 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.

2. Computer resources and access accounts are to be used only for the purpose for which they are assigned and are not to be used for commercial purposes or non-college related activities.

3. All computer software is protected by the federal copyright law and most is proprietary and protected by legal binding agreements in addition to the copyright law. Users are responsible for being aware of and compliant with the licensing restrictions for any software used on any system.

4. Gaston College provides access to outside networks which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material which may be considered offensive or objectionable in nature or content. Gaston College does not assume responsibility for the content of any of these outside networks.

C. Users are expected to comply with legal and ethical standards. Certain behaviors are forbidden, including but not limited to:

1. Damage or disruption to hardware or communications, such as virus creation and propagation.

2. Deletions, examinations, copying or modification of data files belonging to Gaston College or other users without their prior consent.

3. Use of systems and or networks in an attempt to gain unauthorized access to remote systems or to view or capture data.

4. "Spoofing," i.e., unauthorized electronic communications so it appears to be from, or created by, someone else.

5. "Snooping," i.e., unauthorized access to electronic files or information with no substantial College business purpose.

6. It will be understood that some materials retrieved from Internet sites, especially graphics files, are inappropriate for college purposes and offensive to many users. Display of offensive or inappropriate materials on public workstations is expressly forbidden and may result in revocation of computing privileges. Any attempt to create, display, transmit or make accessible threatening, racist, sexist, obscene or harassing language or materials, such as broadcasting unsolicited or sending unwanted mail, is strictly forbidden.

7. Further, it is not permissible to deliberately attempt to damage and/or sabotage institutional computers, computer software or computer networks.

D. Reservations of Rights & Limits of Liability

a. Gaston College reserves all rights in the use and operation of its computer resources, including the right to monitor and inspect computerized files, resources and/or computer support services, or to terminate service at any time and for any reason without notice.

b. The College makes no guarantees or representations, either explicit or implied, that user files and/or accounts are private or secure.

c. The College and its representatives are not liable for any damages and/or losses associated with the use of any of its computer resources or services.

d. The College reserves the right to limit the allocation of computer resources for users, i.e., bandwidth, computer crime, disk space, etc.

E. Electronic Mail

1. Access and Use of Electronic Mail

    a. Only Gaston College faculty, staff, and students and other persons who have received permission under the appropriate College authority are authorized users of the College's electronic mail systems and resources.

    b. The use of any College resources for electronic mail must be related to College business, including academic pursuits. Incidental and occasional personal use of electronic mail may occur when such use does not generate a direct cost for the College. All uses of electronic mail utilizing Gaston College computer resources are subject to the provisions of this policy.

2. Monitoring and Disclosure of Electronic Mail

    a. Gaston College will make reasonable efforts to maintain the integrity and effective operation of its electronic mail systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of electronic communication, the College can assure neither the privacy of an individual user's use of the college's electronic mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

    b. The College will not monitor electronic mail as a routine matter but it may do so to the extent permitted by law as the College deems necessary for purposes of maintaining the integrity and effective operation of the College's electronic mail systems. Any user of the College's electronic mail resources who makes use of an encryption device to restrict or inhibit access to his or her electronic mail must provide access to such encrypted communications when requested to do so under appropriate College authority.

    c. To the extent permitted by law, the College reserves the right to access and disclose the contents of faculty, staff, students', and other users' electronic mail without the consent of the user. The College will do so when it believes it has a legitimate business need including, but not

limited to, those listed below, and only after explicit authorization is obtained from vice president responsible for technology services:

(1) in the course of an investigation triggered by indications of misconduct or misuse
(2) as needed to protect health and safety
(3) as needed to prevent interference with the academic mission, or
(4) as needed to locate substantive information required for College business that is not more readily available by some other means

d. The College will inspect and disclose the contents of electronic mail when such action is necessary to respond to legal processes and to fulfill the College's obligations to third parties.

F. Public Inspection and Archiving of Electronic Mail

a. Electronic mail of students may constitute "education records" subject to the provisions of the federal statute known as the Family Educational Rights and Privacy Act of 1974 (FERPA). The College may access, inspect, and disclose such records under conditions that are set forth in the statute.

b. North Carolina law provides that communications of College personnel that are sent by electronic mail may constitute "correspondence" and, therefore, may be considered public records subject to public inspection under North Carolina General Statutes 121 and 132.

c. Electronic files, including electronic mail, that are considered to be public records are to be retained, archived and/or disposed of in accordance with current guidelines established by the North Carolina Department of Cultural Resources.

G. Violations

a. Violations of this policy will be treated in accordance with college disciplinary procedures for employees and students.

b. Criminal violation will be prosecuted to the fullest extent of the law and may result in the immediate suspension of computing privileges.

History

Issued: 5/16/06, Technology Services Policy only, not included in this policy and procedure manual.
Revised: 6/1/11, added to the Policy and Procedure Manual; prohibited unauthorized "Spoofing" and "Snooping;" banned attempts to damage or sabotage College computers, software, and networks; established guidelines for computer monitoring, inspection, disclosure of computer-related information, and public inspection and archiving of electronic mail; and set forth revised guidelines for violations of the policy.