TECHNOLOGY USE POLICY

BCC POLICY NUMBER 5.10

SOURCE, REFERENCE: NORTH CAROLINA GENERAL STATUTES, ARTICLE 60, "COMPUTER-RELATED CRIME," CHAPTER 14:453, 457; ARTICLE 60 “CYBERBULLYING,” CHAPTER 14:458.1; CHAPTER 132 OF THE NORTH CAROLINA GENERAL STATUTES; AND FEDERAL LAWS, INCLUDING BUT NOT LIMITED TO, COMPUTER FRAUD AND ABUSE ACT OF 1986, COMPUTER FRAUD AND ABUSE ACT 1994, COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1988, COMPUTER SECURITY ACT OF 1990, THE HIGHER EDUCATION OPPORTUNITY ACT OF 2008

REVISION RESPONSIBILITY: VICE PRESIDENT FOR FINANCE AND ADMINISTRATION

COMMENTS: N /A

POLICY STATEMENT:

This policy establishes the responsibilities of all users and acceptable and unacceptable uses of college computers, computing technology, equipment, and networks in support of the administrative and academic functions at Bladen Community College. This policy applies to all employees, students, contractors, visitors or others who use, access or deploy college technology while on any premises, whether leased or owned, As such, computer workstations, equipment, technology and networks may be monitored from time-to-time to ensure compliance.

Overview

Bladen Community College requires lawful use of technology among members of the campus community (employees, students, visitors).

Access to information systems

Access to information systems, computer systems, and computer networks at Bladen Community College is granted to authorize users for the purpose of accessing these systems and networks. Appropriate use of technology is required in order to maintain access to college networks.

Appropriate use

Appropriate use of technology must be ethical, reflect academic honesty and demonstrate restraint in the use of shared resources. Appropriate use must be in compliance with intellectual property right rules; copyright policies; data system security mechanisms; individual rights to privacy (including FERPA), the laws of the state of North Carolina; and, policies established by the State Board of Community Colleges. Acceptable use also requires avoiding acts of cyber bullying, sexual harassment, solicitation, or sending threatening, racist, obscene, unwanted materials or messages.

The college will take all practical measures possible to protect privacy rights. The director of IT shall have the ability to view files and messages on the networks, and make determinations of appropriate or inappropriate use.

1. **Acceptable User Access**
   Authorized users with legitimate educational, administrative, and operational need to access electronic files may do so as part of their duties or assignments. To ensure appropriate use of all technology resources, users shall adhere to the following behaviors/activities.

   a. Use resources only for authorized purposes.

   b. Protect USERIDs and passwords (electronic signatures) from unauthorized use and assume responsibility for any unauthorized use of USERIDs or passwords. Account access granted to an individual user shall not be shared with another user, as each user is responsible for the proper use of their account. Obtaining another user's password or allowing unauthorized access is a violation of this policy**.**

   Users may not expect privacy however in material content sent or received by them over the college's equipment or networks. Information contained on College networks, including but not limited to e-mail, may be subject to inspection under the Public Records Law of North Carolina.

   c. Access only files and data to which authorized access has been given as part of assigned duties or classes.

   d. Use only legal versions of copyrighted software or electronic publications in compliance with vendor license requirements or terms of use policies. Computer and software is generally protected by federal copyright law. Most software is proprietary and protected by legal licensing agreements. Users are responsible for being aware of these protections and agreements, and shall not download, reproduce or distribute copyrighted or licensed materials without legal authorization.

   e. Use technology resources prudently, avoiding monopolizing systems, overloading networks with excessive data or downloads, wasting computer time, excessively connecting to internal or external networks or abusing printing or other related resources.

2. **Unacceptable User Access**
   To ensure acceptable use of all technology resources, users shall not engage in the following behaviors/activities:
   a. Use another person's USERID, password, files, system, or sharing of electronic signature without permission.
   b. Use computer resources to decode passwords or access controlled information.

c. Attempt to circumvent, subvert, or damage system security measures.

d. Engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating computer viruses, disrupting services, or damaging, deleting, or destroying files.

e. Use the college's systems for partisan political activities, such as using electronic mail to solicit support for a political candidate.

f. Make or use illegal copies of copyrighted media files or pirated software or store such copies on college systems, or transmit them over college networks, including peer to peer file sharing.

g. Use college messaging systems, including, but not limited to, campus email systems, learning management systems and college social media sites, for purposes of cyber-bullying, broadcasting unsolicited mass messages, or distribution of unwanted mail.

h. Use system for personal gain unless authorized by the college.

i. Use systems for downloading, sending, or receiving information that contains obscene, indecent, or lascivious material or other material which explicitly or implicitly refers to sexual conduct or for downloading, sending, or receiving information which is bigoted or sexist. The college reserves the right to judge if material meets criteria for the above.

j. Create, modify, execute, or retransmit any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages.

k. Use Bladen Community College's resources for cyber-bullying or any other computer related crimes as outlined in Chapter 14:453, 457; Article 60 "Cyber-bullying of the General Statutes of the General Assembly of North Carolina

l. All networks and technology resources (desktop, laptop and mobile devices) are the property of Bladen Community College, and thereby, subject federal and state laws Pertaining to lawful usage.

Violations

Violations of this policy and guidelines will result in appropriate disciplinary action through established college disciplinary procedures, which may include, but not be limited to, suspension of computing and information system access privileges, suspension, or expulsion, or termination of employment. The college will contact state or federal authorities for prosecution for violation of state or federal laws. Unauthorized users may also be subject to prosecution under relevant state and federal laws.

Liability

Users are responsible for knowledge and compliance with any updates to this document. Current editions will be posted on the college's website. Users are solely responsible for all activity with the respect to their accounts, electronic, communications, and data security.

Approved by the Board of Trustees: 11/26/2013
Revised and Approved by the Board of Trustees - 11/28/2017, effective 01/01/2018