

ADOPTED FEBRUARY 25, 2002  
REVISED AUGUST 22, 2005  
REVISED MARCH 8, 2010

Descriptor Term:  
NETWORK SECURITY

Descriptor Code:  
6.5240

Legal References: G.S. 115C-523, -524; State Board of Education Policy TCS-C-018; Family Educational Rights and Privacy Act, 20 U.S.C. 1232 §; Children's Internet Protection Act Public Law 106-554; Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030 §; National Information Infrastructure Protection Act 1996 Public Law 104-294; Children's Online Privacy Protection Act of 1998; Electronic Communications Privacy Act, 18 U.S.C. 2510-2522 §.

Cross References: 1.6100 Professional and Staff Development; 3.2200 Technology in the Educational Program; 3.3250 NC WISE Password and Workstation Policy; 3.3260 Remote Access Policy; 3.3270 Virus Protection Policy; 3.3280 Security Awareness Policy; 3.4300 School Improvement Plan; 6.5200 Use of Equipment, Materials and Supplies; 6.5210 Use of Equipment, Materials and Supplies; 6.5220 Use of Equipment, Materials and Supplies

Catawba County Schools is dedicated to providing safe and reliable access for network and Internet resources while providing privacy and security for all users. The school system computers, networks and other technological resources support the educational and administrative functions of the school system. Because employees and students depend on these systems to assist with teaching and learning and because sensitive and confidential information may be stored on these systems, system integrity and security is of utmost importance.

#### A. USERS RIGHTS AND RESPONSIBILITIES

All employees and students who use the Catawba County Schools network and computer equipment are subject to all procedures and guidelines stated in board policies, including but not limited to, 3.6140 and 7.1310 and to the student or staff acceptable use policies. Failure to comply with these policies can result in suspension of rights to use the Catawba County Schools network and computer equipment, and other disciplinary actions. Guest users are subject to this policy and the guidelines as stated in the acceptable use policies.

A firewall is between the system's private networks and the Internet to protect the networks. Employees, students, and guests shall not circumvent the firewall. All other forms of Internet access are prohibited. Some protocols may be blocked or redirected for security purposes.

Internet use is monitored and is provided for educational purposes. Users who violate this policy are subject to disciplinary or legal action.

Users are responsible for the backup of their individual workstation data. Designated personnel are responsible for backup of servers and location specific data.

#### B. PRIVACY STATEMENT

Catawba County Schools may collect any information and traffic on any school computer, including but not limited to the following user information: domain name, name, information regarding what pages are

accessed, information volunteered by the person(s) accessing the server(s) such as survey information, email address, site registrations, and preferred means of communication.

Catawba County Schools may not make individual identifying information available to third parties, including business partners and other educational departments or agencies, except as provided by law. At times vendors may offer discounted rates to Catawba County Schools' employees who register information through the Catawba County Schools' servers. Information volunteered by the user may then be passed to the third party offering the discounted service.

Questions or comments sent electronically to an employee of Catawba County Schools may be forwarded to other system employees who are best suited to answer the users' question or comment. This information may not be shared with third parties.

#### C. NETWORK AND INFORMATION SECURITY

Some network resources may require unique identifiers to authenticate the user. These identifiers will be issued by the Information and Technology Department.

For site security purposes and to ensure that service remains available to all users, industry-standard methods will be used to monitor network traffic to identify unauthorized attempts to upload or change information, utilize excessive bandwidth or otherwise cause damage. Security measures will be applied to both wired and wireless networks within the district. Unauthorized attempts to upload information or change information on servers are strictly prohibited and may be punishable by law. In the specific context of this security monitoring, there is not expectation of privacy.

The school system information technology systems are valuable assets that must be protected. To this end, school technology personnel shall evaluate each information technology asset and assign protective controls that are commensurate with the established value of such assets. Appropriate security measures must be in place to protect all information technology assets from accidental or unauthorized use, theft, modification or destruction and to prevent the unauthorized disclosure of restricted information. Network security measures must include an information technology system disaster recovery process. Audits of security measures must be conducted annually.

All personnel shall ensure the protection and security of information technology assets that are under their control.

#### D. SECURITY AWARENESS

The chief technology officer or designee shall provide employees with information to enhance awareness regarding technology security threats and to educate them about appropriate safeguards, network security and information security.

#### E. VIRUS PROTECTION

Virus detection programs and practices must be implemented throughout the school system. The superintendent or designee is responsible for ensuring that the school system network includes current software to prevent the introduction or propagation of computer viruses.

#### F. TRAINING FOR USE OF TECHNOLOGICAL RESOURCES

Users should be trained as necessary to effectively use technological resources. Such training

should include information related to remote access, virus protection, NC WISE, network and information security, and other topics deemed necessary by the superintendent staff development appropriations for technological training in its school improvement plan. The superintendent and chief technology officer should assist schools in coordinating staff development needs as provided in policy 1.6100/7.8000, Professional and Staff Development.

G. ACCESS TO INFORMATION TECHNOLOGY SYSTEMS

1. User ID and Password

All users of information technology systems must be properly identified and authenticated before being allowed to access such systems. The combination of a unique user identification and a valid password is the minimum requirement for granting access to information technology systems. Depending on the operating environment, information involved and exposure risks, additional or more stringent security practices may be required as determined by the superintendent or chief technology officer. The chief technology officer or designee shall establish password management capabilities and procedures to ensure the security of passwords.

2. NC WISE

The chief technology officer or designee shall ensure that any school system computers utilizing the NC WISE application pursuant to State Board of Education Policy TCS-C-018 adhere to requirements of the NC WISE Password and Workstation Policy, including provisions related to the user identification, password and workstation security standards. Employees must follow such standards for all computers used to access the NC WISE system, including the employee's personal computer.

3. Remote Access

The superintendent and chief technology officer may grant remote access to authorized users of the school system's computer systems. The chief technology officer or designee shall ensure that such access is provided through secure, authenticated and carefully managed access methods.