

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. NETWORK AND INFORMATION SECURITY**

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.

**B. SECURITY AWARENESS**

The technology director 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. Security breaches that compromise the integrity of the school system's data or network shall be reported immediately to the Director of Technology, who shall investigate and take any appropriate action.

**C. 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.

**D. TRAINING FOR USE OF TECHNOLOGICAL RESOURCES**

Users should be trained as necessary to use technological resources effectively and in a manner that maintains the security of the network infrastructure and ensures compliance with state and federal law and regulations. 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 or technology director.

---

Training may be conducted as part of the technology-related professional development program (see policy 3220, Technology in the Educational Program).

## **E. 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, selected in compliance with guidelines developed by the Technology Department and published on the school system website, is the minimum requirement for granting access to information technology systems. Such guidelines shall also be provided to principals, school-based technology contacts and site-based technology facilitators.

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 technology director. The technology director or designee shall establish password management capabilities and procedures to ensure the security of passwords. Technology personnel shall not request passwords from users.

### **2. NC WISE**

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

### **4. Confidentiality**

Employees shall be assigned a network user ID and password only after reading and signing the *Access to Confidential Information* release. It shall be the responsibility of supervisors to maintain signed releases and verify that each individual accessing information is properly trained and aware of confidentiality requirements.

Employees shall not transfer confidential data electronically without using appropriate encryption technologies, which shall be specified by the Director of Technology.

The superintendent shall have the authority to adopt any necessary procedures recommended by the Technology Department regarding the use of technology-related services and equipment. Such procedures shall be published on the school system website.

Legal References: G.S. 115C-523, -524; State Board of Education Policy TCS-C-018

Cross References: Professional and Staff Development (policy 1610/7800), Technology in the Educational Program (policy 3220), Internet Safety (policy 3226/4205), Technology Responsible Use (policy 3225/4312/7320), School Improvement Plan (policy 3430), Use of Equipment, Materials and Supplies (policy 6520)

Other References: NC WISE Password and Workstation Standard (available at [http://www.ncwise.org/documents/training\\_group/docs/Security/WISE\\_schl\\_SecurityAdministration.pdf](http://www.ncwise.org/documents/training_group/docs/Security/WISE_schl_SecurityAdministration.pdf))

Adopted: November 20, 2012