

# **TECHNOLOGY IN THE EDUCATIONAL PROGRAM**

*Date Reviewed/Approved: 3/03/2008*

*Policy Number: 3220*

---

*Rescinds Policy Number:*

*Issued: 3/03/2008*

---

The board strives to incorporate the use of technology in the educational program in order to enhance instructional opportunities, appeal to different learning styles and meet the educational goals of the board.

The Director of Technology and Media will develop a local school system technology plan that meets state requirements and submit the plan to the board for approval. Once approved by the board, the Director of Technology and Media will take all steps necessary to gain approval of the plan by the State Board of Education. After the plan is approved by the State Board, all state funds spent for any aspect of school technology will be used to implement the technology plan.

Schools are encouraged to develop strategies for using technology to improve student success. The strategies should be included in the school improvement plan if it requires the transfer of funds or otherwise relates to any mandatory or optional components of the school improvement plan. Expenditures of state funds must be consistent with the school district's technology plan.

The Director of Technology and Media is expected to establish relationships with businesses and seek grants and other funding sources in an effort to acquire technology for the educational program.

## **A. SELECTION OF TECHNOLOGY MATERIAL**

All technological resources, including computers, software and communication lines, must be purchased and used in a manner consistent with applicable law and board policy, including laws and policies related to copyright, public records, bidding and other purchase requirements, staff duties and standards for student behavior.

Technology materials will meet or exceed the following factors before they will be considered for implementation.

1. Technologies must relate to or help implement the North Carolina Standard Course of Study or the programs of the school district.
2. Technologies must relate to the current use of learning and instructional management technologies in the school.
3. Any technologies purchased must be compatible with the condition of the network. The technology director will set minimum standards for technological resources that are purchased or donated. Upgrading, hardware conditions and similar requirements will be maintained to the highest standards.
4. Staff development must be made available to implement technologies so that the benefits of the technologies will be maximized.
5. Staffing requirements must be adequate to operate the technologies and to maintain the equipment.
6. There must be a budget available for the technologies.

## **B. DEPLOYMENT OF TECHNOLOGY TO SCHOOLS**

The Director of Technology and Media will oversee the development of the school district's technology deployment plan. The plan will be designed to ensure organized, effective and efficient means of deploying new hardware and software. The Director of Technology and Media will develop procedures that outline the strategy of the technology deployment plan.

**C. NETWORK AND INFORMATION SECURITY**

The school district information technology systems are valuable assets that must be protected. To this end, school technology personnel will 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 will include an information technology system disaster recovery process. Audits of security measures will be conducted annually.

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

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.

**D. VIRUS PROTECTION**

Virus detection programs and practices shall be implemented throughout the school district. The Director of Technology and Media is responsible for ensuring that the school district network includes current software to prevent the introduction or propagation of computer viruses.

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

Users should be trained as necessary to effectively use the 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 or technology director. Schools should identify any staff development appropriations for technological training in their school improvement plans. The superintendent and technology director should assist schools in coordinating staff development needs as provided in board policy 1610/7800, Professional Development and Assistance.

**F. ACCESS TO INFORMATION TECHNOLOGY SYSTEMS; USER ID AND PASSWORDS; NC WISE**

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 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 technology director. The technology director or his/her designee will establish password management capabilities and procedures to ensure the security of passwords.

The technology director or his/her designee will ensure that any school district computers utilizing the NC WISE application pursuant to State Board of Education Policy EEO-C-018 adheres 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.

The Director of Technology and Media may grant remote access to authorized users of the school district's computer systems. The technology director or designee will ensure that such access is provided through secure, authenticated and carefully managed access methods. Orange County employee passwords (e.g., email, Web and calendar) used to access systems and applications shall be in accordance to the NC Wise Security Administration policy.

Legal References: Communication Act of 1934, *as amended*, 47 U.S.C. §609; G.S. 115C-102.6C, -522, -522.1; G.S. 147-33.111, G.S. 115C-105.27; State Board of Education Policy EEO-C-018

Cross References: Copyright Compliance (policies 3230/7330), NC Wise Security Administration Policy, Public Records (policy 5070), Citizenship and Character Education (policy 3530), Staff Responsibilities (policy 7300), Professional Development and Assistance (policy 1610/7800), Gifts and Bequests (policy 8220)

Adopted: