TECHNOLOGY IN THE EDUCATIONAL PROGRAM

In alliance with state school technology goals, the Board is committed to establishing and supporting 21st century information and communications technology systems to foster globally competitive, healthy and responsible students. The Board recognizes the benefits of digital and technology-enabled teaching and learning resources that provide the ability to easily customize curriculum, provide access to current information and enable access to quality materials at a lower cost than traditional materials. To that end, the Board intends to move to classroom digital and technology-enabled teaching and learning resources that are aligned with the Common Core State and North Carolina Essential Standards as they become available. In addition, to the extent funding permits, the Board will endeavor to ensure that all students have access to personal digital and technology-enabled teaching and learning devices to foster the 21st century skills necessary for future-ready learners.

The Board expects that information and communications technologies will be integrated across the curriculum and used to support student achievement. Such technologies will also be used to support programs and activities that promote safe schools and healthy and responsible students. The curriculum committee should provide suggestions in the curriculum guides referenced in policy 3115, Curriculum and Instructional Guides, for integrating technological resources (as defined in Section A below) into the educational program. School administrators and teachers are encouraged to develop additional strategies for integrating technological resources across the curriculum and utilizing the power of technology to improve learning outcomes while making more efficient use of resources. The strategies should be included in the school improvement plan if they require the transfer of funds or otherwise relate to any mandatory or optional components of the school improvement plan.

The Superintendent or designee 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. ACQUISITION, USE AND SUPPORT OF TECHNOLOGIES

All technological resources, including computers, software and communication services, must be acquired and used in a manner consistent with applicable law and Board policy, including laws and policies related to selection of instructional resources, copyright, public records, bidding and other acquisition requirements, staff duties and standards for student usage.

Technologies will meet or exceed the following standards before they will be considered:

1. Technologies must relate to or help implement the Common Core State and North Carolina Essential Standards 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 acquired must be compatible with the network. The technology director will set minimum standards for acquiring, updating and maintaining all system-wide technological resources. Staff development must be made available to implement technologies so that the benefits of the technologies will be maximized.

4. Staffing requirements must be adequate to operate the technologies and to maintain the equipment.

5. Staffing requirements must be adequate to operate the technologies and to maintain the equipment.

B. DEPLOYMENT OF TECHNOLOGIES TO SCHOOLS

The Superintendent or designee will oversee the deployment of the school district's technologies. Procedures will be developed that outline the strategies for deployment.

C. BRING YOUR OWN TECHNOLOGY (BYOT) INITIATIVE

The Superintendent is authorized to investigate and develop a plan to allow staff and students the option to use their personal electronic devices in place of or along with their school system assigned devices. The plan should address, at a minimum, the instructional use of personal devices, compatibility requirements, access limitations or requirements, content filtering, security and other issues as recommended by the technology director. The plan should assign personal responsibility to the user for repair and replacement of damaged or stolen devices and for any data or other charges arising from use of a personal device. The plan should require a written agreement for the use of personal technology devices from each student and staff member who wishes to participate in the BYOT initiative. The plan should ensure that students who are unable to bring in outside technology will be able to access and utilize school equipment so that no student is excluded from instruction due to lack of access to technology.

D. NETWORK AND INFORMATION SECURITY

Asheville City School's computer networks, equipment and resources are owned by the School System and are provided primarily to support the academic and administrative functions of the School System. Because employees and students depend on these systems to assist with teaching and learning, system integrity is of utmost importance and these valuable assets must be protected. To this end, the Instructional Technology Department shall evaluate each information technology asset and develop, implement and maintain appropriate user security measures 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.

E. 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.

F. VIRUS PROTECTION

Virus detection programs and practices shall be implemented throughout the school district. The Superintendent or his/her designee is responsible for ensuring that the school district network includes current measures to prevent the introduction or propagation of computer viruses.

G. TRAINING FOR USE OF TECHNOLOGICAL RESOURCES

Users shall be trained as necessary to effectively use the technological resources. Such training should include information related to remote access, virus protection, network and information security and other topics deemed necessary by the Superintendent or technology director. Schools should identify any staff development needs for technological training in their school improvement plans. The Superintendent and technology director should assist schools in coordinating staff development training as provided in Board policy 7800, Professional Development and Assistance.

H. ACCESS TO INFORMATION TECHNOLOGY SYSTEMS

1. User ID's and Passwords

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 in consultation with the District MTAC, shall establish password management capabilities and procedures to ensure the security of the network and shall publish, on the School System website, the regulations and guidelines established for users to select and implement a unique username and password. These regulations and guidelines shall be provided to principals, school technology contacts, and site-based technology facilitators. All ACS users shall be responsible for maintaining the security and privacy of their own network security credentials.

2. Remote Access

The Superintendent and technology director 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.

Legal References: Communication Act of 1934, as amended, 47 U.S.C. § 609; G.S. 115C-102.6C -522; G.S. 147-33.111; State Board of Education Policy EEO-C-018 Cross References: Professional and Staff Development (policy 7800)

Cross References: Copyright Compliance (policies 3230), School Improvement Plan (policy 3430), Standards of Expected Student Behavior (policy 4310), Public Records (policy 5070), Use of Computers (policy 6523), Staff Responsibilities (policy 7300), Professional Development and Assistance (policy 7800)

Adopted: May 11, 1998
Revised: October 2, 2006
August 5, 2013