Policy Code: 3220 Technology in the Educational Program

In alliance with the North Carolina Digital Learning Plan, the Board is committed to establishing and supporting effective digital teaching and learning practices supported by contemporary information and communications technology systems to foster globally competitive students prepared for modern life. The board recognizes the benefits of digital and technology-enabled and -enhanced teaching and learning resources that provide the ability to make data more accessible, personalize learning, 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 supports classroom digital and technology-enabled, and -enhanced teaching and learning resources that are aligned with the current statewide instructional standards. 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 skills necessary for future-ready learners.

The board expects that information and communications technologies will be integrated seamlessly across the curriculum and used to support student achievement and to prepare students to be successful in college, in careers, and as globally engaged, productive citizens. All curriculum committees 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 personalize learning and 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 components of the school improvement plan.

The superintendent shall oversee development of the school system's digital teaching and learning vision as part of the school district's strategic plan and a yearly action plan that aligns to the vision. The development and ongoing review of the vision and action plan will include various stakeholders such as curriculum leaders, teachers, administrators, students and parents, and representatives from technology services, instructional technology, finance, and other departments as required. The action plan will include adequate data privacy protections to secure student data and will take into account the level of out-of-school Internet access for students.

The superintendent may establish relationships with businesses and nonprofits, and seek grants and other funding sources in an effort to acquire additional technological resources for the educational program and to support continuous out of school internet access for students.

A. Selection of Technological Resources

Technological resources are information and communication technologies including, but are not limited to, the following: (1) hardware, including both fixed and mobile technologies and devices such as desktop computers, laptops, netbooks, tablets, e-readers, smartphones, and gaming devices; (2) software , including cloud-based and web-based applications, programs, and platforms; (3) network and telecommunications systems and services; (4) Internet access; (5) multimedia equipped classrooms; (6) computer classrooms and laboratories; and (7) other existing or emerging mobile communication systems. All technological resources 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, accessibility for students with disabilities, staff duties, and standards for student behavior.

Technological resources must meet or exceed the following standards before they may be considered for implementation.

3220

1. Technological resources must support the current statewide instructional standards or the programs of the school system.

2. Technological resources must support the current use of learning and instructional management technologies in the school.

3. Technological resources must be compatible with the condition of the network and other infrastructure resources. The Executive Director of Technology shall set minimum standards for technological resources that are purchased or donated. Upgrading, hardware conditions, and similar requirements must be maintained to the highest standards.

4. There must be sufficient staff to operate and maintain the technological equipment, programs and systems.

5. There must be adequate funds budgeted to implement and support the technological resources and to train instructional staff to use the resources to improve educational outcomes.

Procurement of technological resources should be done in collaboration with teachers and technical support staff, as appropriate. Whenever possible, a pilot period to test the resource should occur prior to full purchase.

B. Deployment of Technology to Schools

The superintendent shall oversee the development of the school system's technology deployment and refresh plan. The plan will be designed to ensure organized, effective, efficient, and sustainable means of deploying and maintaining technology resources and will establish appropriate refresh/replacement cycles. The superintendent, or designee, shall develop procedures that outline the strategy of the technology deployment and refresh plan.

C. Network and Information Security

The school district information technology systems are valuable assets that must be protected as referenced in Network Security Policy 6524. 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 Executive Director of Technology 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 superintendent or designee is responsible for ensuring that the school district network includes current software to prevent the introduction or propagation of computer viruses.

3220

E. Bring Your Own Technology (BYOT) Initiative

The superintendent is authorized to investigate and develop regulations to allow staff and students the option to use their personal electronic devices in place of or along with their school system assigned devices as referenced in policy 4318 Use of Wireless Communication Devices. The plan should address, at a minimum, the instructional use of personal devices, compatibility requirements, access limitations or requirements, content filtering, security, equity, and other issues as recommended by the Executive Director of Technology. 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 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.

F. Electronic Communication and Other Collaborative Tools

The superintendent is authorized to permit instructional personnel to incorporate email, social networking sites, blogs, wikis, video sharing sites, podcasts, video conferencing, online collaborations, instant messaging, texting, virtual learning environments, and/or other forms of direct electronic communications or Web 2.0 applications for educational purposes to the extent the superintendent deems appropriate and in accordance with policy 7335, Employee Use of Social Media. The superintendent shall establish parameters and rules for use of these tools and shall require instruction for students in how to use such tools in a safe, effective, and appropriate way. Instructional personnel shall make all reasonable attempts to monitor student online activity and shall otherwise comply with the requirements of policy 3225/4312/7320, Technology Responsible Use, when using these tools.

G. Technology-Related Professional Development

The superintendent will implement a program of professional development for digital teaching and learning that prepares the administrators, teachers, coaches, school library media coordinators and technical support staff to utilize digital tools and resources in accordance with the N.C. Digital Learning Competencies for Teachers and Administrators. Professional development shall emphasize technology integration and continuous improvement, including the use of ongoing technology-integrated online-learning activities throughout the course of study and the provision of personalized learning. Professional development shall also address the ethical, legal, and practical issues related to social networking and mobile devices in the classroom and other topics deemed necessary by the superintendent or technology director. To the extent possible, job-specific professional development opportunities should be made available, as well as professional development that is personalized to meet the needs of individual staff.

School improvement teams should identify any staff development appropriations for technology-related professional development in their school improvement plans. The superintendent and Executive Director of Technology should assist schools in coordinating staff development needs as provided in policy 1610/7800, Professional and Staff Development.

H. Access to Information Technology Systems; User ID and Passwords; Student Information System

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

3220

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 Executive Director of Technology or designee will establish password management capabilities and procedures to ensure the security of passwords.

The Executive Director of Technology or designee will ensure that any school district computers utilizing the Student Information System application pursuant to State Board of Education Policy EEO-C-018 adheres to requirements of the Student Information System 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 Student Information System system, including the employee's personal computer.

The superintendent and Executive Director of Technology may grant remote access to authorized users of the school district's computer systems. The Executive Director of Technology or designee will ensure that such access is provided through secure, authenticated and carefully managed access methods.

Legal References: G.S. 115C-522, -528; 143B-1341; State Board of Education Policy SBOP-018

Cross References: Professional and Staff Development (policy 1610/7800), Curriculum and Instructional Guides (policy 3115), Technology Responsible Use (policy 3225/4312/7320), Internet Safety (policy 3226/4205), Copyright Compliance (policy 3230/7330), School Improvement Plan (policy 3430), Integrity and Civility (policy 4310), Use of Wireless Communication Devices (policy 4318) Public Records (policy 5070/7350), Network Security (policy 6524), Staff Responsibilities (policy 7300), Employee Use of Social Media (policy 7335), Gifts and Bequests (policy 8220)

Other Resources: North Carolina Digital Teaching and Learning Competencies for Teachers and Administrators and The North Carolina Digital Learning Plan (2022)

Issued: June 1997

Revised: 2/5/04, 7/20/06, 5/21/15, 5/1/17, 4/12/2023

Chapel Hill-Carrboro Schools