

Technological resources, including computers, other electronic devices, programs, networks and the Internet, provide opportunities to enhance instruction, appeal to different learning styles and meet the educational goals of the board. Through the school system's technological resources, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current and in-depth information.

Use of technological resources should be integrated into the educational program. Technological resources should be used in teaching the North Carolina Standard Course of Study and in meeting the educational goals of the board. The curriculum committee should provide suggestions for using technological resources in the curriculum guides as provided in policy 3115, Curriculum and Instructional Guides. Teachers are encouraged to further incorporate the use of technological resources into their lesson plans.

The superintendent shall ensure that school system computers with Internet access comply with federal requirements regarding filtering software, Internet monitoring and Internet safety policies. The superintendent shall develop any regulations and submit any certifications necessary to meet such requirements.

**A. REQUIREMENTS FOR USE OF TECHNOLOGICAL RESOURCES**

Before using the Internet, all students must be trained about appropriate on-line behavior. Such training must cover topics such as cyberbullying and interacting with others on social networking websites and in chat rooms.

Anyone who uses school system computers or electronic devices or who accesses the school network or the Internet at an educational site must comply with the requirements listed below. All students and employees must receive a copy of this policy annually. Before using school system technological resources, students, their parents and employees must sign a statement indicating that they understand and will strictly comply with these requirements. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful misuses may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

1. School system technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to activities that support learning and teaching. Use of school system technological resources for commercial gain or profit is prohibited.
2. Under no circumstance may software purchased by the school system be copied for personal use.
3. Students and employees must comply with all applicable board policies,

administrative regulations, and school standards and rules in using technological resources. All applicable laws, including those relating to copyrights and trademarks, confidential information, and public records, apply to technological resource use. Any use that violates state or federal law is strictly prohibited.

4. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing or considered to be harmful to minors.
5. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
6. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personally identifiable, private or confidential information, such as the home address or telephone number, of themselves or fellow students. In addition, school employees must not disclose on the Internet or on school system websites or web pages any personally identifiable information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4700, Student Records. Users also may not forward or post personal communications without the author's prior consent.
7. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software or computer networks. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance. Users must scan any downloaded files for viruses.
8. Users may not create or introduce games, network communications programs or any foreign program or software onto any school system computer, electronic device or network without the express permission of the technology director or designee.
9. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems or accounts.
10. Users are prohibited from using another individual's computer account. Users may not read, alter, change, execute or delete files belonging to another user without the owner's express prior permission.
11. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem

to other users. Any user identified as a security risk will be denied access.

12. Teachers shall make reasonable efforts to supervise a student's use of the Internet during instructional time.
13. Views may be expressed as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.

**B. RESTRICTED MATERIAL ON THE INTERNET**

Before a student may use the Internet for any purpose, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material. The parent and student must sign a consent form acknowledging that the student user is responsible for appropriate use of the Internet and consenting to monitoring by school system personnel of the student's e-mail communication and use of the Internet.

The board is aware that there is information on the Internet that is not related to the educational program. The board also is aware that the Internet may provide information and opportunities to communicate on subjects that are not suitable for school-age children and that many parents would find objectionable. School system personnel shall take reasonable precautions to prevent students from having access to inappropriate materials, such as violence, nudity, obscenity or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that the Internet service provider or technology personnel have installed a technology protection measure that blocks or filters Internet access to audio or visual depictions that are obscene, that are considered pornography or that are harmful to minors. School officials may disable such filters for an adult who uses a school-owned computer for bona fide research or another lawful educational purpose. School system personnel may not restrict Internet access to ideas, perspectives or viewpoints if the restriction is motivated solely by disapproval of the ideas involved.

**C. PRIVACY**

No right of privacy exists in the use of technological resources. School system administrators or individuals designated by the superintendent may review files, monitor all communication, and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School system personnel shall monitor on-line activities of individuals who access the Internet via a school-owned computer.

**D. PERSONAL WEBSITES**

The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school system or individual school names, logos or trademarks without permission.

1. Students

Though school personnel generally do not monitor students' Internet activity conducted on non-school system computers during non-school hours, when the student's on-line behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy (see the student behavior policies in the 4300 series).

2. Employees

All employees must use the school system network when communicating with students about any school-related matters. Thus, employees may not use personal websites or on-line networking profiles to post information in an attempt to communicate with students about school-related matters.

Employees are to maintain an appropriate relationship with students at all times. Employees are encouraged to block students from viewing personal information on employee personal websites or on-line networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. If an employee creates and/or posts inappropriate content on a website or profile and it has a negative impact on the employee's ability to perform his or her job as it relates to working with students, the employee will be subject to discipline up to and including dismissal. This section applies to all employees, volunteers and student teachers working in the school system.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 6777; G.S. 115C-325(e), -391

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Copyright Compliance (policy 3230/7330), Web Page Development (3227/7322), Student Behavior Policies (all policies in the 4300 series), Public Records – Retention, Release and Disposition (policy 5070/7350), Use of Equipment, Materials and Supplies (policy 6520), Network Security (policy 6524), Staff Responsibilities (policy 7300)

Adopted: January 3, 2012