The board provides its students and staff access to a variety of technological resources. These resources provide opportunities to enhance learning, improve communication within the school community and with the larger global community, 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.

The board intends that students and employees benefit from these resources while remaining within the bounds of safe, legal and responsible use. Accordingly, the board establishes this policy to govern student and employee use of school system technological resources. This policy applies regardless of whether such use occurs on or off school system property, and it applies to all school system technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks.

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. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

The use of school system technological resources, including access to the Internet, is a privilege, not a right. Individual users of the school system's technological resources are responsible for their behavior and communications when using those resources. Responsible use of school system technological resources is use that is ethical, respectful, academically honest and supportive of student learning. Each user has the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette. General student and employee behavior standards, including those prescribed in applicable board policies, the Code of Student Conduct and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school system computers or electronic devices or who accesses the school network or the Internet using school system resources must comply with the

additional rules for responsible use listed in Section B, below. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive.

Before using the Internet, all students must be trained about appropriate online behavior. The training will cover topics such as cyberbullying and interacting with others on social networking websites as provided in policy 3226/4205, Internet Safety.

All students and employees must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Before using school system technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements and acknowledging awareness that the school system uses monitoring systems to monitor and detect inappropriate use of technological resources. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges (see Section E below). Willful misuses may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

Technological resources as a part of all instructional resources shall be evaluated and selected by the media/technology staff working collaboratively with teachers. Policies which apply to instructional resources also apply to technological resources.

B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School system technological resources are provided for school-related purposes only. Acceptable uses of such technological resources are limited to responsible, efficient and legal activities that support learning and teaching. Use of school system technological resources for other purposes such as for commercial gain or profit, joining a mailing list or assisting in a political campaign or fund raising for non-school related activities is prohibited. Student personal use of school system technological resources for amusement or entertainment is also prohibited. Because some incidental and occasional personal use by employees is inevitable, the board permits infrequent and brief personal use by employees so long as it occurs on personal time, does not interfere with school system business and is not otherwise prohibited by board policy or procedure.

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. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Code of Student Conduct

4. No student or employee may use school system networks or technological resources to send email/electronic messages to multiple users on issues not school-related. This use of email/electronic messages is considered spam and may result in disciplinary action and revocation of privileges. Electronic messages are defined to include texting by cell phones, interactive chat, or any other written communication sent using electronic devices.

5. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, 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, abusive or considered to be harmful to minors.

6. The use of anonymous proxies to circumvent content filtering is prohibited.

7. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.

8. No user of technological resources shall use the school system networks or computing devices to harass, insult, defame, threaten, attack or bully others.

9. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

10. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, students must not reveal personal identifying information, or information that is private or confidential, such as the home address or telephone number, credit or checking account information or social security number of themselves or fellow students. For further information regarding what constitutes personal identifying information, see policy 4705/7825, Confidentiality of Personal Identifying Information. In addition, school employees must not disclose on school system websites or web pages or elsewhere on the Internet any personally identifiable, private or confidential 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.

11. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks or data of any user connected to school system technological resources. 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. Users may not download files or change software settings on computers or other electronic devices unless instructed to do so by the media/technology staff. Only designated media/technology staff may install software on district computers.

12. 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.

13. 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.

14. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also have permission from the teacher or other school official.

15. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.

16. Employees shall not use passwords or user IDs for any data system (e.g., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.

17. 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.

18. Students may not use technological resources during class time without permission from the teacher. Teachers and principals shall be responsible for adopting classroom procedures regarding use of technological resources during class time and making students aware of these procedures. Teachers shall supervise a student's use of the Internet and technological resources during instructional time.

19. Views may be expressed on the Internet or other technological resources as representing the view of the school system or part of the school system only with prior approval by the superintendent or designee.

20. Users may not connect any personal or donated computing equipment to school system networks or computing equipment without permission from the technology director or designee. Users may not reconfigure or move any equipment without permission and assistance from the technology director or designee.

C. RESTRICTED MATERIAL ON THE INTERNET

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The board recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain that is not related to the educational program. Nevertheless, school system personnel shall take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, including violence, nudity or graphic language that does not serve a legitimate pedagogical purpose. The superintendent shall ensure that technology protection measures are used as provided in policy 3226/4205, Internet Safety. The board is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service). Filtering is intended to ensure access to instructional content relevant to the NCSCOS and to content which does not disrupt the educational process or violate board policies or laws.

D. PARENTAL CONSENT

The board recognizes that parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parent must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent and student must consent to the student's independent access to the Internet and to monitoring of the student's Internet activity and e-mail communication by school personnel.

In addition, in accordance with the board's goals and visions for technology, students may require accounts in third party systems for school related projects designed to assist students in mastering effective and proper online communications or to meet other educational goals. Parental permission will be obtained when necessary to create and manage such third party accounts.

E. PRIVACY

Students, employees, visitors and other users have no expectation of privacy in anything they create, store, send, delete, receive or display when using the school system's network, devices, Internet access, email system or other technological resources owned or issued by the school system, whether the resources are used at school or elsewhere, and even if the use is for personal purposes. Users should not assume that files or communications created, transmitted or displayed using school system technological resources or stored on servers or on the storage mediums of individual devices will be private. The school system may, without notice, (1) monitor, track and/or log network access, communications and use; (2) monitor and allocate fileserver space; and (3) access, review, copy, store, delete or disclose the content of all user files, regardless of medium, the content of electronic mailboxes and system outputs, such as printouts, for any lawful purpose. Such purposes may include, but are not limited to, maintaining system integrity, security or functionality, ensuring compliance with board policy and applicable laws and regulations, protecting the school

system from liability and complying with public records requests. School system personnel shall monitor on-line activities of individuals who access technology resources via a school-owned device or school provided email.

By using the school system's network, Internet access, email system, devices or other technological resources, individuals consent to have that use monitored by authorized school system personnel as described in this policy.

F. USE OF PERSONAL TECHNOLOGY ON SCHOOL SYSTEM PROPERTY

The technology director in cooperation with the media/technology staff will establish rules as to whether and how personal technology devices (including, but not limited to smart phones, tablets, laptops, etc.) may be used on campus. Students' devices are governed also by policy 4318, Use of Wireless Communication Devices. The school system assumes no responsibility for personal technology devices brought to school.

G. 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 devices 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

   Employees are to maintain an appropriate relationship with students at all times. Employees must 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 and student teachers working in the school system.

   Whether an employee chooses to personally participate in a blog, wiki, online social network or any other form of electronic online publishing or discussion, is his or her decision. However, material that employees post on social networks that is available

to those in the school community must reflect the professional image applicable to the employee's position and not impair the employee's capacity to maintain the respect of students and parents/guardians or impair the employee's ability to serve as a role model for children. It is inappropriate to use e-mail, text messaging, instant messaging, social networking tools, cell phones or any other forms of electronic communication to discuss with a student a matter that does not pertain to curriculum-related activities. Personal web sites, cell phones and any other form of personal electronic publishing by employees must not use photos or movies taken at school or contain pictures of students or staff.

Employees are prohibited from using electronic communications to establish personal relationships with students that are unprofessional and thereby inappropriate. Examples of unprofessional relationships include, but are not limited to: employees fraternizing or communicating with students as if employees and students were peers such as writing personal letters or e-mails; personally texting or calling students, or allowing students to make personal calls to them unrelated to homework, class work, or other school-related business; sending inappropriate pictures to students; discussing or revealing to students personal matters about their private lives or inviting students to do the same; and engaging in sexualized dialogue, whether in person, by phone, via the Internet or in writing. An employee who posts on social networking sites inappropriate personal information, including, but not limited to, provocative photographs, sexually explicit messages, abuse of alcohol, drugs or anything students are prohibited from doing, must understand that if students, parents or other employees obtain access to such information, the employee may be subject to disciplinary action after investigation by school and school system officials.

Employees must not use personal electronic communications or personal social networking tools to share confidential information about students or any specific information about students that would violate the Family Educational Rights and Privacy Act.

3. Volunteers

Volunteers are to maintain an appropriate relationship with students at all times. Volunteers are encouraged to block students from viewing personal information on volunteer personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. An individual volunteer's relationship with the school system may be terminated if the volunteer engages in inappropriate online interaction with students.

H. REVOCATION OF PRIVILEGES

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. School system and individual school guidelines for student behavior apply. Computer networks, technological resources and the Internet are provided to

help students to meet the goals of the curriculum as directed by instructional staff. Access to these network services will be provided to students who agree to act in a considerate and responsible manner and abide by the guidelines for appropriate use. Students and employees who violate board policy or regulations on the use of school system technological resources may be subject to the revocation of certain privileges.

I. DISCLAIMER

The board makes no warranties of any kind, whether express or implied, for the service it is providing. The school system will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions, whether caused by the school system's or the user's negligence, errors or omissions. Use of any information obtained via the Internet is at the risk of the user. The school system specifically disclaims any responsibility for the accuracy or quality of information obtained through its Internet services.

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) (applicable to career status teachers), -325.4 (applicable to non-career status teachers)

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Internet Safety (policy 3226/4205), Web Page Development (policy 3227/7322), Copyright Compliance (policy 3230/7320), Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700), Confidentiality of Personal Identifying Information (policy 4705/7825), 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: December 13, 2010

Revised: March 29, 2012; January 28, 2013; June 23, 2014; January 26, 2015