

The board provides its students and staff access to a variety of technological resources that provide opportunities to enhance learning and improve communication within the school community and with the larger global community. 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 the use of technological resources should be integrated into the educational program and 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 students 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.

#### **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. 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 the use of the Internet and other school technological resources.

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 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. 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.

## B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School system technological resources are provided for school-related purposes. 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 commercial gain or profit 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 procedures.
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 laws, including those relating to copyrights and trademarks, confidential information, and public records. 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 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.
5. The use of anonymous proxies to circumvent content filtering is prohibited.
6. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.
7. Users of technological resources may not post information that could be disruptive, cause damage, or endanger students or staff.
8. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
9. 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. 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.
10. 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.
11. 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. Users may not change settings on technological resources without the express permission of the technology director or designee.

12. 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.
13. Users are prohibited from using another individual’s ID or password for any technological resource without permission from the individual. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner’s express prior permission.
14. Employees shall not use passwords or user IDs for any data system (e.g., NCWISE, CECAS, time-keeping software, etc.) for an unauthorized or improper purpose.
15. 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.
16. Teachers shall make reasonable efforts to supervise a student’s use of the Internet during instructional time.
17. 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.

#### **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. 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, and are responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g. 3G, 4G service).

#### **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 parents 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 e-mail communication by school personnel.

## **E. PRIVACY**

No right of privacy exists in the use of technological resources. Users should not assume that files or communications created or transmitted using school system technological resources or stored on services or hard drives of individual computers will be private. 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.

## **F. 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**

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),

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Internet Safety (Policy 3226/4205), Copyright Compliance (policy 3230/7330), Web Page Development (policy 3227/7322), Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700), Public Records (policy 5070), Use of

---

---

Equipment, Materials and Supplies (policy 6520), Staff Responsibilities (policy 7300)

Adopted: June 28, 2000

Revised: April 2, 2002 effective with the 2002-2003 school year

Replaced: January 4, 2011

Revised: December 11, 2012

**EMPLOYEE/SUBSTITUTE EMPLOYEE AGREEMENT**  
**INTERNET IN THE EDUCATIONAL PROGRAM**

As a user of the Onslow County Schools computer network, I have read and hereby agree to comply with Board Policy 3225/7320, Technology Responsible Use. I further acknowledge that I have no expectation of privacy in the use of any school computer; that if I engage in incidental personal use, I will use only my Onslow County Schools-assigned email program to communicate on; and that I will not use or attempt to use any non-school sanctioned internet email service. This agreement will remain in effect until terminated in writing.

I understand that any violation of Board Policy 3225/7320, Technology Responsible Use, shall result in loss of access privileges and may result in disciplinary action, up to and including dismissal.

**Employee Name (Print)** \_\_\_\_\_

**Work Location** \_\_\_\_\_

**Signature** \_\_\_\_\_ **Date** \_\_\_\_\_

**VOLUNTEER AGREEMENT**  
**INTERNET IN THE EDUCATIONAL PROGRAM**

**As a user of the Onslow County Schools computer network, I have read and hereby agree to comply with Board Policy 3225/7320, Technology Responsible Use. I further acknowledge that I have no expectation of privacy in the use of any school computer; that if I engage in incidental personal use, I will use only my Onslow County Schools-assigned email program to communicate; and that I will not use or attempt to use any non-school sanctioned internet email service. This agreement will remain in effect until terminated in writing.**

**I understand that any violation of Board Policy 3225/7320, Technology Responsible Use, shall result in loss of access privileges and may result in my removal from the volunteer program.**

**Volunteer Name (Print)** \_\_\_\_\_

**Volunteer Location** \_\_\_\_\_

**Signature** \_\_\_\_\_ **Date** \_\_\_\_\_

**STUDENT/PARENT AGREEMENT**  
**INTERNET IN THE EDUCATIONAL PROGRAM**

As a user of the Onslow County Schools computer network, I have read and hereby agree to comply with Board Policy 3225/7320, Technology Responsible Use. I further acknowledge that I have no expectation of privacy in the use of any school computer; that if I engage in incidental personal use, I will use only my Onslow County Schools-assigned email program to communicate; and that I will not use or attempt to use any non-school sanctioned internet email service. This agreement will remain in effect until terminated in writing.

I understand that any violation of Board Policy 3225/7320, Technology Responsible Use, shall result in loss of access privileges and may result in disciplinary action.

**Student Name (Print)** \_\_\_\_\_

**School** \_\_\_\_\_ **Grade** \_\_\_\_\_

**Signature** \_\_\_\_\_ **Date** \_\_\_\_\_

As the parent/guardian of the above student, I grant permission for this student to access networked computer services such as electronic mail and the internet. I have read and agree to Board Policy 3225/7320, Technology Responsible Use. I understand that I may be held responsible for violations by this student. This agreement will remain in effect until terminated in writing.

**Parent/Guardian Name (Print)** \_\_\_\_\_

**Signature** \_\_\_\_\_ **Date** \_\_\_\_\_