

ACCEPTABLE USE/INTERNET SAFETY POLICY *Policy Code: 3225/7320*

The Internet/School Network provides a unique opportunity to enhance global instruction, appeal to different learning styles, and meet the educational goals of the Wilkes County Board of Education. Through the Internet/School Network, users can observe events as they occur around the world, interact with others on a variety of subjects, and acquire access to current, varied, and in-depth information.

The Internet should be used in teaching the North Carolina Essential Standards and in meeting the educational goals of the Board of Education. Teachers will integrate the Internet into their curriculum.

REQUIREMENTS FOR USE OF THE INTERNET AND SCHOOL NETWORK

The use of the Internet is a privilege, not a right. Inappropriate use of the Internet may result in limitation or cancellation of user privileges and appropriate disciplinary action. Before using the Internet, all students shall receive training about appropriate on-line behavior. Such training shall include cyber bullying, interacting with others on social networking websites and in chat rooms, and cyber bullying awareness and response.

Users of the Internet, including staff and students, must comply with the following requirements.

- The Internet/School Network is provided primarily for school-related purposes. No right of privacy exists in any communication on the Internet or the School Network. The school district monitors and archives employee e-mail messages for 3 years in compliance with Board of Education policies, applicable laws, and regulations. Electronic information is subject to inspection or deletion by authorized members of the Technology Department.
- Students/Staff must meet all standards of expected online behavior and comply with all Board of Education policies, applicable laws, and regulations.
- All staff will model and promote ethical use of technology.
- Teachers will educate students in using appropriate online behavior including Internet safety while using social networking sites and chat rooms as well as the dangers of cyber bullying.
- No person may use school equipment, software, or email for personal gain, profit, or to promote a political position. Wilkes County Schools does not support the advertisement of any product or the promotion of any political agenda via electronic communications. It is the responsibility of school administrators to address such violations (see consequences section).
- No user of the Internet, electronic device, and/or any storage device may engage in creating, requesting or transmitting offensive, fraudulent, pornographic, harassing, obscene, or vulgar images or documents. Messages with derogatory or inflammatory remarks concerning religion, ethnicity, national origin, sexual preference, etc. will not be transmitted or posted.
- Users will not participate in cyber bullying.

ACCEPTABLE USE/INTERNET SAFETY POLICY *Policy Code: 3225/7320*

- Users will not create or transmit chain letters via e-mail.
- All laws and Board of Education policies apply for all users, including those relating to copyright/trademarks, confidential information and public records. Information electronically transmitted or stored is subject to the same copyright laws as govern non-electronic data. The intellectual property of others will be granted the respect afforded copyrighted materials.
- Teachers will supervise and monitor students' use of computers and other technologies.
- Including children under their care before and after school hours and on teacher workdays.
- Accessing programs and websites not appropriate for educational use are prohibited. Students will not participate in Internet instant message activities, visit chat rooms, access personal e-mail accounts (unless it is a curriculum-related requirement) or participate in any activity that may cause harm to themselves or others.
- Teachers and students may use age appropriate Web 2.0 tools for collaboration. Teachers are responsible for reviewing websites' terms of use for age restrictions, and compliance with the Children's Online Privacy Protection Act for students under age 13. (See the Web 2.0 Policy 3223)
- Users will not attempt to gain unauthorized access to programs, websites, network file space, or computer equipment. Attempting to disable or circumvent system filtering software is prohibited. Promoting, advocating, or participating in hacking is strictly prohibited. It is the responsibility of the principal to enforce these policies (see consequences section).
- Users will not maliciously attempt to harm or destroy hardware, software, data, or transmit computer viruses or other malware.
- Unauthorized release, use, and/or distribution of personal information is prohibited. Passwords and other personal information will not be shared or posted in a conspicuous location. Users will not attempt to log in to any system or software using credentials other than their own.
- Users will not change settings on school equipment unless authorized by the Technology Department.
- Disrupting the network is prohibited.
- Users will not download or upload software or files unless authorized by the Director of Technology.
- Users will not save to the network in unauthorized locations. Locations will be designated by Wilkes County Schools' Network Engineer.

ACCEPTABLE USE/INTERNET SAFETY POLICY *Policy Code: 3225/7320*

- Personal laptops, computers, or iPads, may not be on school premises without written permission from the Director of Technology. Wilkes County Schools cannot ensure personal computers are free from viruses and malware. In order to protect computers, systems, and networks belonging to Wilkes County Schools from harm, no personal computer use of any kind will be allowed for students and/or staff. Wilkes County Schools cannot ensure compliance with the federal Child Internet Protection Act (CIPA) for personal computers; therefore, personal computer use will not be allowed for students, faculty, or staff.
- Opinions expressed as representing the view of the school district must receive prior approval by the superintendent or his or her designee.
- Wilkes County Schools is not responsible for individual employee maintained web pages or contents. Employees must follow all Board of Education policies for school web pages.

RESTRICTED MATERIAL

All users are responsible for appropriate use of technology. Parents, students, and employees should be aware that the school district monitors use of computers. Before a student may use the Internet, the legal parent/guardian should be aware of the possibility that the student could obtain access to inappropriate material. The school district only supports individual students using filtered, e-mail accounts and age appropriate Web 2.0 tools for instructional purposes. The school district has established technology measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, harmful to minors. The Board of Education shall enforce the operation of these technology measures.

In the event a legal parent/guardian chooses not to allow their child to participate in web based activities, it is the responsibility of the parent to notify the school principal in writing annually. Permission is not necessary for student participation in required online testing.

The Board of Education is aware that information is available on the Internet that is not related to the curriculum. The Board of Education also is aware that the Internet offers information and opportunities to communicate on subjects that are not suitable for school-age children. Filtering software is used to guard against accidental or intentional access to inappropriate Internet locations. It should be understood that no filtering software is 100% effective. The school district will take reasonable precautions to prevent students from having access to inappropriate materials which do not serve legitimate pedagogical concerns. These inappropriate materials include but are not limited to violence, nudity, obscenity, prejudice, or graphic language. The system does not condone the use of controversial or offensive materials. The school district will not limit access to the Internet solely for the purpose of restricting political ideas or social perspectives. The user is ultimately responsible for his or her activity on the Internet. Teacher supervision is required when students are using computers and other technologies.

ACCEPTABLE USE/INTERNET SAFETY POLICY *Policy Code: 3225/7320*

Confidential student information will be handled according to the guidelines set forth by the Family Educational Rights and Privacy Act (FERPA). If sensitive electronic data is housed online or electronically, great care will be taken to prohibit unauthorized viewing, editing or duplication of files electronically or otherwise.

All school system employees and students will follow the guidelines set forth in the Children's Internet Protection Act (CIPA), the Neighborhood Children's Internet Protection Act (NCIPA) and the Broadband Data Improvement Act (BDIA).

CONSEQUENCES

Student offenses will result in one or more of the following at the discretion of school administrators

- Notification to legal parent/guardian
- Financial compensation for damages
- Limitation or loss of user privileges
- Suspension or other disciplinary action as deemed appropriate by the school administrator
- Appropriate authorities will be notified of illegal activities
- For any act of student vandalism, appropriate disciplinary action will be taken in accordance with the policies of the Board of Education. Appropriate law enforcement authorities may be notified. Students will be held financially responsible for damage repair or replacement costs.

Employee offenses will result in one or more of the following at the discretion of school or district officials

- Private consultation with school or district officials
- Letter of reprimand placed in personnel folder
- Financial compensation for damages
- Limitation or loss of user privileges
- Any other disciplinary action deemed appropriate by school officials
- Appropriate authorities will be notified of illegal activities
- For any act of staff vandalism, appropriate disciplinary action will be taken in accordance with the policies of the Board of Education. Appropriate law enforcement authorities may be notified. Staff will be held financially responsible for damage repair or replacement costs.

CONTRACTS

All students and staff must electronically accept the Requirements for the Use of the Internet and School Network within the Acceptable Use/Internet Safety policy online before gaining access to the Internet. The Acceptable Use/Internet Safety policy will be included annually in the student policy handbook and electronic employee policies.

ACCEPTABLE USE/INTERNET SAFETY POLICY *Policy Code: 3225/7320*

Legal References: U.S. Const. amends. I; 17 U.S.C. 100 et seq.; Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; G.S. 115C-391, -325(e), PL 106-554, SBE EEO-C-018, SB 991, 2004, GS 115c-98, GS 115c-398, GS 115c-106

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Copyright Complaint (policy 3230/7330), Standards of Expected Student Behavior (policy 4310), Public Records (policy 5070), Staff Responsibilities (policy 7300), Student Records (policy 4700), Web 2.0 (3223), Hardware (3221), Software (3222)

Adopted: May 17, 2004

Revised: November 7, 2005, July 7, 2008, June 7, 2010, January 31, 2011, December 5, 2011, June 16, 2014