

Descriptor Term:
TECHNOLOGY ACCEPTABLE USE AND INTERNET SAFETY --
STUDENTS

Descriptor Code:
3.6140/4.2050

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:

In the 21st Century, technology tools and electronic resources are an integral part of a comprehensive educational program. Through these, both students and staff are able to extend classrooms beyond the four walls of their schools, enriching experiences and communicating on a global level.

Computers, other electronic devices, programs, networks and the Internet support instruction, appeal to different learning styles and meet the educational goals of the board.

Use of technological resources should be integrated and infused into the system's educational program. Technological resources should be used in teaching the North Carolina Standard Course of Study and in incorporating national curriculum standards. They should also be an integral part of a comprehensive system communication program, facilitating exchange of information.

It is the policy of the board to:

1. prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;
2. prevent unauthorized access and other unlawful online activity;
3. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
4. comply with the Children's Internet Protection Act [Pub. L. No. 106-544 and 47 USC 254(h)].

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

The use of school system technological resources, such as computers and other electronic devices, networks, and the Internet, is a privilege, not a right. 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. Before using school system technological resources, students 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 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 4.8000 Student Records. Users also may not forward or post personal communications without the author's prior consent.
7. Users are prohibited from cyberbullying and other harassing activities conducted through school networks.

Harassment includes, but is not limited to, slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, visual depictions, pranks, or verbal conduct relating to an individual that (a) have the purpose or effect of creating an intimidating, hostile or offensive environment; (b) have the purpose or effect of unreasonable interfering with an individual's work or school performance; or (c) interfere with school operations.

8. Users who intentionally or negligently damage computers, computer systems, electronic devices, software or computer networks are guilty of vandalism. 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.

9. 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 chief technology officer or designee.
10. 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. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors is forbidden by the Children’s Internet Protection Act.
11. 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.
12. Users are prohibited from connecting any personal technologies to system owned and maintained local, wide, or metro area networks without permission of the board. These include computers, wireless access points and routers, printers, iPods, smartphones, PDAs.
13. 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.
14. It is the responsibility of school administrators and staff to supervise student use of the internet during instructional time as well as enforcing this policy.
15. 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.
16. While the board undertakes comprehensive security measures, appropriate use of school networks and the Internet ultimately remains the responsibility of the user. Therefore, the board is not responsible for loss of or corrupted data, service interruptions or delays, obtaining information of poor quality, or other inaccurate information.

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. The benefits from the valuable information and interaction available to students, however, outweigh the disadvantages of the possibility that students may find inappropriate material. 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.

Though school personnel generally do not monitor students' Internet activity conducted on non-school system computers during non-school hours, when a 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 policy 4.3600 Code of Student Conduct.

E. DISCIPLINARY ACTION

Disciplinary action for students who violate this policy shall be consistent with the policy 4.3600 Code of Student Conduct.