

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

Descriptor Code:
3.6142/7.1310

Legal References:

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. These resources should be used in teaching the North Carolina Standard Course of Study and in incorporating national curriculum standards. They also support valid business uses and provide for efficient work-related communication. This policy defines employees' proper conduct and responsibilities while using any school system electronic information resources. Employees are defined as all teachers, administration, and staff. This policy also applies to any other users who are expressly authorized by the board to use electronic information resources, including, but not limited to, board members, contractors, consultants, and temporary workers. Electronic information resources are defined as all computer equipment, peripherals, or other hardware that is owned or leased by the school system; user accounts (e.g. email, Novell, Active Directory); and any software licensed to the board.

Users must acknowledge that access and use of all board electronic resources is considered a privilege and not a right. Misuse of these resources may result in loss of this privilege as well as possible disciplinary or legal action.

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. APPROPRIATE USE

All users are expected to exercise good judgment, use computer resources in a professional manner, and adhere to this policy and all applicable laws and regulations.

Use of electronic information resources is expected to be related to the school system's goals of educating students and/or conducting school system business. The board recognizes, however, that some personal use is inevitable, and that incidental and occasional personal use that is infrequent or brief in duration is permitted so long as it occurs on personal time, does not interfere with the employee's work or school system business, and is not otherwise prohibited by board policy or regulations, procedures, or applicable law.

B. HARDWARE AND SOFTWARE

The board's comprehensive network is comprised of servers, computers, printers, peripherals, switches, routers, software and other devices. These resources are installed and maintained by members of the board's Information and Technology Department. Staff members shall not attempt to perform installation and maintenance without permission of the board's Technology Department.

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.

Software is licensed to the board by a large number of vendors and may have specific license restrictions regarding copying or using a particular program. Users must obtain permission from the Information and Technology Department prior to copying or loading school system software onto any computer, whether the computer is privately owned or is a board computer.

The use of software not owned or authorized by the board on any school system computers (including laptops, desktops, and the network) is discouraged. Prior to loading any software not owned or authorized by the board, an employee must receive express permission from the Information and Technology Department. The use of such software will be subject to any restrictions specified by the software license and to any restrictions imposed by the Technology Department. All software must be legally licensed by the user or the board prior to loading onto school system equipment. The unauthorized use of and/or copying of software is illegal.

The board's network may not be used for downloading entertainment software or other files not related to the mission and objectives of the board. This prohibition pertains to freeware, shareware, copyrighted commercial and non-commercial software, and all other forms of software and files not directly related to the instructional and administrative purposes of the board.

C. PROHIBITED USES

The following uses are prohibited uses of school system computers:

1. Commercial Use: Using school system computers for personal or private gain, personal business, or commercial advantage is prohibited.
2. Political Use: Using school system computers to advocate, directly or indirectly, for or against legislation, a ballot proposition and/or the election of any person to any office is prohibited.
3. Illegal or Inappropriate Use: Using school system computers for illegal, harassing,

vandalizing, or inappropriate purposes, or in support of such activities, is prohibited.

Illegal activities are any violations of federal, state, or local laws and include, but are not limited to, copyright infringement and/or illegal file sharing; committing fraud; threatening another person; or intentionally engaging in communications for the purpose of abusing, annoying, threatening, terrifying, harassing, or embarrassing another person.

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 unreasonably interfering with an individual's work or school performance; or (c) interfere with school operations.

Vandalism is any attempt to harm or destroy an operating system, hardware, application software, or data.

Inappropriate use is any violation of other provisions of this policy and includes, but is not limited to, using another person's ID or password; plagiarizing; accessing, producing, storing, posting, sending, displaying, or viewing inappropriate or offensive material, including pornographic, obscene, discriminatory, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually suggestive language or images, or images of exposed private body parts; and accessing material advocating illegal acts or violence, including hate literature.

4. Unauthorized Use: School system computers may only be used by staff and students, and others expressly authorized by the Information and Technology Department.
5. Disruptive Use: Board computers may not be used to interfere with or disrupt other users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising ("spam"), propagation of computer viruses, distribution of large quantities of information that may overwhelm the system (chain letters, network games, or broadcasting messages), and any unauthorized access to or destruction of school system computers or other resources accessible through the network ("cracking" or "hacking"). Disruptive use may also be considered inappropriate and/or illegal.

The following are considered disruptions and are also prohibited: posting personal or private information about the user or other people on the Internet; arranging or agreeing to meet with someone the user has met online for purposes other than official school business; attempting to gain unauthorized access to the board's network; posting information that could be disrupting, cause damage, or endanger students or staff; and accessing chat-rooms or instant messaging software, unless for a valid educational purpose or official school business.

D. STAFF WEBSITES

The board provides numerous avenues through which teachers can facilitate their instructional programs. SharePoint, the board's web portal, provides each teacher with his/her own web site where instructional information should be posted. The board's XServe enables teachers to set up wikis and blogs to promote interaction with students. The board's Virtual Learning Environment (VLE) portal is the approved venue for hosting system-created online courses and supplemental content. All content posted on these sites remains the intellectual property of the board.

There are numerous outside web sites where employees can bookmark and compile information to support their instructional goals. These sites are not appropriate venues to serve as substitutes for the employees' of the board's SharePoint, XServe, and VLE servers. Information posted on outside sites becomes the property of the site and the employee no longer has ownership or control of content. For this reason employees may not use these sites to post information for students.

The board recognizes that social networking sites can provide an important avenue of communication between staff, students, and parents. An employee who wants to utilize these sites must set up a board account that is separate from the employee's personal social networking site. Staff may use these system-specific sites to post announcements for parents, students and the community; they may not use these sites for posting instructional information.

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 online 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/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.

E. COMPLIANCE WITH POLICY

This policy is applicable to all employees of the board and refers to all electronic information resources whether individually controlled, shared, stand-alone, or networked. Disciplinary action for employees shall be consistent with board policies and practices. Violation of this policy may constitute cause for revocation of access privileges, suspension of access to school system computers, dismissal and/or appropriate disciplinary or legal action.

F. STUDENT MONITORING RESPONSIBILITIES

School administrators and staff are responsible for reading the Student Acceptable Use Policy and for enforcing the policy for any and all students at the site in which they work. Administrators and staff must supervise student use of electronic information resources and technology equipment in a manner that is appropriate to the students' age and circumstances of use.

G. MONITORING/NO EXPECTATION OF PRIVACY

The board's electronic information resources, the Internet, and use of email are not inherently secure or private. Employees shall have no expectation of privacy while using school system electronic information resources. The board reserves the right to search data or email stored on all school-owned or leased computers or other electronic information resources at any time for any reason. The board reserves the right to monitor employees' use of school system electronic information resources and to take appropriate disciplinary action based on the employees' inappropriate or illegal use or use that is in violation of this policy. The board reserves the right to disclose any electronic message to date to law enforcement officials, and under some circumstances, may be required to disclose information to law enforcement officials or other third parties, for example, in response to a document production request made in a lawsuit involving the board or pursuant to a public records disclosure request.

H. SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. Employees are responsible for reporting information security violations to appropriate personnel. Employees should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the board's network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access.

Users of the board's technology equipment are expected to respect school system property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school system is responsible for any routine maintenance or standard repairs to school system computers.

I. NO WARRANTIES

The board makes no warranties of any kind, whether express or implied, for the electronic information it is providing. The board will not be responsible for any damages suffered by users, including a loss of data resulting from delays, non-delivery, service interruptions, or any other cause. The board will not be responsible for any claims, losses, damages, costs, or other obligations arising from the unauthorized use of school system electronic information resources. Use of any information obtained via the Internet is at the user's risk. The board specifically denies any responsibility for the accuracy or quality of information obtained through its service. Users are responsible for any losses sustained by the board resulting from the user's intentional misuse of the school system's electronic information resources.

J. APPLICATION OF PUBLIC RECORDS LAW

All information created or received for work purposes and stored on or contained in the school system's computer resources or electronic data files is subject to public disclosure unless an exception to the Public Records Law applies. This information may be purged or destroyed only in accordance with the applicable records retention schedule and the State Division of Archives regulations. Staff email accounts will be archived for a minimum of three years.

K. EMPLOYEE AGREEMENT FORM

An Employee Acceptable Use Policy Agreement Form, developed by the school system, must be signed by the employee before access is permitted and an email account is assigned. An employee's acceptance of the Agreement is considered a condition of employment and refusal to sign may result in discipline up to and including dismissal.