

The board provides its students and staff access to a variety of technological resources. These resources 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 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.

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 as provided in policy 5.24, 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 misuse 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 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 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 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 laws, including those relating to copyrights/trademarks, confidential information and public records. Any use that violates state or federal laws is strictly prohibited. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in policy 5.3, Student Conduct.
4. No user of the 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, 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 send electronic communications fraudulently (i.e. by misrepresenting the identity of the sender).

8. Users must respect the privacy of others. When using email, chat rooms, blogs, or other forms of electronic communication, students must not reveal personally identifying information, or information that is private or confidential, such as 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 web sites or webpages or elsewhere on the Internet any personally identifiable, private or confidential information concerning students (including names, addresses or pictures) except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or applicable board policy. Users also may not forward or post personal communications without the author's prior consent.

9. 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.

10. 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.

11. 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 or computer systems or accounts.

12. Users are prohibited from using another individual's ID or password for any technological resource.

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

14. Employees shall not use passwords or user ID's for any data system (e.g. NCWISE, CECAS, time-keeping software, etc.) for an authorized or improper purpose.

15. If a user identifies a security problem on a technological resource, he/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 will make reasonable efforts to supervise a student's use of the Internet during instructional time.

17. Views may not be expressed on the internet or other technological resources as representing the view of the school system or part of the school system unless approval is given by the superintendent or his or her designee.

C. RESTRICTED MATERIAL

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 student may access or obtain. Nevertheless, the school system personnel shall take reasonable precautions to prevent students from accessing materials and information that is obscene, pornographic, or otherwise

harmful to minors, such as violence, nudity, or graphic language which does not serve a legitimate pedagogical purpose. The superintendent shall ensure that technology protection measures are used as provided in policy 5.24, Internet Safety, and are disabled or minimized only when permitted by law and board policy. 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).

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 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 or transmitted using school system technological resources or stored on services or hard drives of individual computers will be private. The school system may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and allocate files server 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 online activities of individuals who access the Internet via a school-owned device.

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

Each principal may establish rules for his or her school site as to whether and how personal technology devices (including, but not limited to smart phones, tablets, laptops, etc.) may be used on campus. Students are required to use school provided "guest" network to access internet for all school related instructional activities. Students' devices are governed also by policy 5.3.4.7. The school system assumes no responsibility for personal technology devices brought to school. The instructional activities in this policy are in accordance with the Federal CIPA and Protecting Children in the 21st Century Act.

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 online 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.

2. Employees

Employees' personal websites are subject to policy 3.20 (1), Employee Use of Social Media.

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.

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)

Adopted: March 4, 2008

Revised: May 7, 2013

Revised: May 7, 2015