

The board provides its students and staff access to a variety of technological resources. These resources provide opportunities to enhance learning and student achievement and to improve communication with 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.

The use of school system technological resources is a privilege, and use in violation of this policy may result in revocation of the privilege.

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 addition 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.

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. 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 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. 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. Plagiarism of Internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Code of Student Conduct.
3. Under no circumstances may software purchased by the school system be copied for personal use.
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, 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 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 home address or telephone number, credit or checking account information or social security number of themselves or fellow students. For further information regarding what constitutes personal identifying information, see policy 4705/7825, Confidentiality of Personal Identifying Information. In addition, school personnel 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 permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or board policy 4700, Student Records. 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, computer systems, or accounts.
12. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users shall not demonstrate the problem to other users. Any user identified as a security risk shall be denied access.
13. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also have permission from the teacher or other school official.
14. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.
15. Employees shall not use passwords or user IDs for any data system (e.g., NCWISE, CECAS, time-keeping software, etc.) for an authorized or improper purpose.
16. Teachers shall make reasonable efforts to supervise students' 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.
18. All employees are required to use the BCS network or approved off-network sites when creating websites for any and all educational and work related postings or

communications with students.

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 materials and information that are obscene, pornographic, or otherwise harmful to minors, including content that contains 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 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).

Users are ultimately responsible for their activity on the Internet. The board will not be responsible for any damages, including loss of data resulting from delays or service interruptions. 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 technological resources.

D. PARENTAL CONSENT

The board believes that the benefits to students from access to the Internet, in the form of information resources and opportunities for communication and collaboration, exceed any disadvantages. However, 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. Parents or legal guardians may deny access to their child at any time through completion of a Parental Request to Deny Access Form. The form is available upon request from your child's school. It may also be downloaded from the forms section of the district's Internet website. Parent's requests to deny access are effective only for the current school year and do not carry over into the child's next school year.

Completion of the form prohibits an individual student's unfettered personal access to the Internet. Students that have had their individual Internet access denied are still able to participate in staff-led activities that contain Internet content. Students who are denied Internet access are not protected from viewing Internet content in use by other students. Students that have been denied a BCS email account but not Internet access may have access to e-mail accounts from other service providers or Internet locations.

1. School administrators are responsible for ensuring that each student's parent or legal guardian is made aware that parents or guardians have the option to deny their child's access to the Internet, e-mail, or both.
2. Schools are free to incorporate the content of Parental Request to Deny Access form into custom school forms, but may not change the content therein.
3. Conflicts on the delivery of Internet based curriculum or other similar issues due to the student not having Internet access must be resolved between the parent and the school principal.

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

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 4000 series).

2. Employees

Employees' personal websites are subject to policy 7335, 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 volunteers' personal websites or on-line 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.

G. USER AGREEMENT

A user may access school system technological resources only after returning to the school administration or designee a completed BCS Responsible Use of Technology and Internet Safety Agreement that includes a user's signature. The user's signature signifies the user's understanding of and agreement to adhere to board policies, administrative procedure adopted by the superintendent that implement this policy, and any additional procedures imposed by local school administration.

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), -390.2

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 (3227/7322), Student Behavior Policies (all policies in the 4300 series), Student Records (policy 4700), Confidentiality of Personal Identifying Information (policy 4705/7825), Public Records – Retention, Release and Disposition (policy 5070/7350), Use of Equipment, Materials and Supplies (policy 6520), Network Security (policy 6524), Staff Responsibilities (policy 7300), Employee Use of Social Media (policy 7335)

Adopted: August 16, 2011

Revised: March 23, 2015