The board provides students and staff access to a variety of technological resources. These resources provide opportunities to enhance learning, appeal to different learning styles, improve communication within the school community and with the larger global community, and achieve the educational goals established by the board. 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 expected to be exercised in an appropriate and responsible manner. 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 school technological resources, including access to the Internet.

In addition, anyone who uses school system computers or electronic devices accesses the school's electronic storage or network, or connects to the Internet using school system-provided access 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.

All students must be trained about appropriate online behavior as provided in policy 3226/4205, Internet Safety.

Failure to adhere to the requirements of this policy will result in disciplinary action, including revocation of user privileges. Willful misuse may result in criminal prosecution under applicable state and federal law, disciplinary action for students, and/or adverse personnel action for employees.

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 unless approved for special situations by the teacher or school administrator. 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. Unless authorized by law to do so, users may not make copies of software purchased by the school system. Under no circumstance may software purchased by the school system be copied for personal use.

3. Users must comply with all applicable laws, board policies, administrative regulations, and school standards and rules, including those relating to copyrights and trademarks, confidential information, and public records. 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.

4. Users must follow any software, application, or subscription services terms and conditions of use.

5. 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, profane, pornographic, harassing, abusive, or considered to be harmful to minors.

6. Users must not circumvent fire walls. The use of anonymous proxies to circumvent content filtering is prohibited.

7. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.

8. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

9. Users must respect the privacy of others.

    a. Students must not reveal any personally identifying, private, or confidential

information about themselves or fellow students when using email, chat rooms, blogs, or other forms of electronic communication. Such information includes, for example, a person's home address or telephone number, credit or checking account information, or social security number. For further information regarding what constitutes personal identifying information, see policy 4705/7825, Confidentiality of Personal Identifying Information.

b. School employees 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 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 4700, Student Records.

c. Users may not forward or post personal communications without the author's prior consent.

d. Students may not use school system technological resources to capture audio, video, or still pictures of other students and/or employees in which such individuals can be personally identified, nor share such media in any way, without consent of the students and/or employees and the principal or designee. An exception will be made for settings where students and staff cannot be identified beyond the context of a sports performance or other public event or when otherwise approved by the principal.

10. 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, including by streaming audio or video for non-instructional purposes. Users may not disable antivirus programs installed on school system-owned or issued devices.

11. 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.

12. 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.

13. Users are prohibited from using another individual's ID or password for any technological resource or account without permission from the individual. Sharing of an individual's ID or password is strongly discouraged. If an ID or password

must be shared for a unique classroom situation, students must 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., the state student information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.

16. If a user identifies or encounters an instance of unauthorized access or another security concern, he or she must immediately notify a teacher, school system administrator, or the technology director or designee. Users must not share the problem with other users. Any user identified as a security risk will be denied access.

17. It is the user's responsibility to back up data and other important files.

18. Employees shall make reasonable efforts to supervise students' use of the Internet during instructional time.

19. 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.

20. Users who are issued school system-owned and -maintained devices for home use (such as laptops, Chromebooks, etc.) must adhere to any other reasonable rules or guidelines issued by the superintendent or technology director for the use of such devices.

21. Without permission by the board, users may not connect any person technologies such as laptops, workstations and printers, wireless access points and routers, etc. to a district owned and maintained local, wide or metro area network. Connection of personal devices such as iPods, smartphones, PDAs and printers is permitted but not supported by Montgomery County Schools. 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).

22. Those who use district owned and maintained laptops must also follow these guidelines:

    a. Keep the laptop secure and damage free

    b. Use the provided protective case at all times.

    c. Do not loan out the laptop, charger or cords.

d. Do not leave the laptop in your vehicle.

e. Do not leave the laptop unattended.

f. Do not eat or drink while using the laptop or have food or drinks in close proximity to the laptop.

g. Do not allow pets near the laptop.

h. Do not place the laptop on the floor or on a sitting area such as a chair or couch.

i. Do not leave the laptop near table or desk edges.

j. Do not stack objects on top of the laptop.

k. Do not leave the laptop outside.

l. Do not use the laptop near water such as a pool.

m. Do not check the laptop as luggage at the airport.

n. Back up data and other important files regularly, Montgomery County Schools Technology Department will at times perform maintenance on the laptops by imaging. All files not backed up to server storage space or other storage devices will be deleted during this process.

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 material and information that is obscene, pornographic, or otherwise harmful to minors, including 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 using a cellular network to connect a personal device to the Internet.

D. 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, transmitted, or displayed using school system technological resources or stored on servers, the storage mediums of individual devices, or on school managed cloud services will be private. Under certain circumstances, school officials may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the board, in response to a public records request, or as evidence of illegal activity in a criminal investigation.

The school system may, without notice, (1) monitor, track, and/or log network access, communications, and use; (2) monitor and allocate fileserver space; and (3) access, review, copy, store, delete, or disclose the content of all user files, regardless of medium, the content of electronic mailboxes issued by the school system, and system outputs, such as printouts, at any time 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, electronic devices, email system, devices, or other technological resources, individuals consent to have that use monitored by authorized school system personnel as described in this policy.

E. USE OF PERSONAL TECHNOLOGY ON SCHOOL SYSTEM PROPERTY

Users may not use private WiFi hotspots or other personal technology on campus to access the Internet outside the school system's wireless network. Each principal may establish rules for his or her school site as to whether and how other personal technology devices (including, but not limited to smart phones, tablets, laptops, etc.) may be used on campus. Students' devices are governed also by policy 4318, Use of Wireless Communication Devices. Use of personal technology devices is also subject to any rules established by the superintendent under a bring your own device plan authorized by Section C of policy 3220, Technology in the Educational Program, and for employees, policy 3228/7323, Use of Personal Technology to Conduct School Business. The school system assumes no responsibility for personal technology devices brought to school.

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 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 to the extent consistent with law (see the student behavior policies in the 4300 series).

2. Employees

   Employees' personal websites are subject to policy 7335, Employee Use of Social Media. Employees may not use their personal websites to communicate with students, as prohibited by policy 7335 and policy 4040/7310, Staff-Student Relations.

3. Volunteers

   Volunteers are to maintain appropriate relationships 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.

G. USE AGREEMENTS

All students, parents, and employees will be informed annually of the information in this policy. Prior to using school system technological resources, students and employees must agree to comply with the requirements of this policy and consent to the school system's use of monitoring systems to monitor and detect inappropriate use of technological resources. In addition, the student's parent must consent to the student accessing the Internet and to the school system monitoring the student's Internet activity and electronic mailbox issued by the school system.

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. 7131; G.S. 115C-325(e) (applicable to career status teachers), -325.4 (applicable to non-career status teachers)

Cross References: Curriculum and Instructional Guides (policy 3115), Technology in the Educational Program (policy 3220), Internet Safety (policy 3226/4205), Web Page Development (policy 3227/7322), Use of Personal Technology to Conduct School Business (policy 3228/7323), Copyright Compliance (policy 3230/7330), 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 1, 2005
Updated: April 6, 2009
Updated: January 12, 2012
Updated: January 14, 2013
Updated: December 8, 2014
Updated: May 4, 2015
Updated: December 5, 2016
Updated: January 10, 2022