TECHNOLOGY RESPONSIBLE USE

Date Reviewed/Approved: 02/26/2018 *Policy Number*: 3225/7320

Rescinds Policy Number: *Issued*: 10/04/2004,12/06/2004,03/03/2008,07/07/2011, 06/22/2012,04/13/2015,01/23/2017

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, externally hosted storage and applications, 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. General student and employee behavior standards, including those prescribed in applicable Board policies, the Employee Code of Ethics, 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, networks or electronic devices or who accesses the school network or the Internet using school system resources must comply with the 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 Board Policy.

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 use system provided methods to indicate that they understand and will strictly comply with these requirements and acknowledging awareness that the school system uses monitoring systems to monitor and detect inappropriate use of technological resources. Failure to adhere to the requirements in this policy will result in disciplinary action. Willful misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCE

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. Because some incidental and occasional personal use is inevitable, the Board permits infrequent and brief personal use so long as it occurs on personal time, does not interfere with school system business, instructional activities, 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, unless permitted by the vendor and approved by the Superintendent or his/her designee.

3. 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.

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 information including but not limited to 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.

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 engage in network or internet activities fraudulently (such as by misrepresenting or impersonating the identity of the sender or another party).

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 the 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 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 Board Policy. Users 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 generate, modify, manage or otherwise store district or school data, including but not limited to information related to operational documentation or student work, on devices or repositories outside of district control, except to temporarily make a copy of such data. Any such temporary copying of such data shall ensure full adherence to federal, state and district privacy and public records laws.

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. Users are prohibited from using another individual's ID or password or access any district device or system logged in with account credentials other than those authorized by HR and assigned to them by IT specifically. Exceptions apply to IT personnel who may need to access devices for troubleshooting purposes. In these instances, IT strongly prefers the individual whose credentials are being used in troubleshooting to be present during IT's work on the device.

13. "Generic" or multi-user accounts are prohibited, except where allowed by the Superintendent or their designee

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 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.

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

18. 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.

19. Users are required to physically secure their device when unattended through the use of password lock, logging off the computer, and otherwise physically securing the device.

20. Users may not connect personal devices, or any devices not owned and managed by district IT to district managed networks, wired or wireless, that are not specifically designated for guest use.

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 Board Policy 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 Internet activity and 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, transmitted, or displayed using school system technological resources or stored on servers or on the storage mediums of individual devices will be private. 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, 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. Notwithstanding this section, the school system will comply with the laws protecting confidential student and staff records where required.

F. USE OF PERSONAL TECHNOLOGY ON SCHOOL SYSTEM PROPERTY

The Superintendent or his/her designee may establish rules as to whether and how personal technology devices (including, but not limited to smart phones, tablets, laptops, etc.) may be used on campus. The school system assumes no responsibility for personal technology devices brought to school. Any permitted use of electronic devices will be subject to Board policy.

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 applicable law and policy.

3. Volunteers

   Volunteers are to maintain appropriate interactions 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.