**TECHNOLOGY ACCEPTABLE USE** *Policy Code:* **4312/7320/3225**

The board provides its scholars 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’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 scholars 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 scholar and employee use of school technological resources. This policy applies regardless of whether such use occurs on or off school property, and it applies to all school 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.

1. **Expectations for Use of School Technological Resources**

The use of school technological resources, including access to the Internet, is a privilege, not a right. Individual users of the school’s technological resources are responsible for their behavior and communications when using those resources. Responsible use of school technological resources is use that is ethical, respectful, academically honest, and supportive of scholar 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 scholar and employee behavior standards, including those prescribed in applicable board policies, the Code of Scholar Conduct, and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school computers or electronic devices or who accesses the school network or the Internet using school 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 scholars must be trained about appropriate online behavior as provided in policy 3226/4205, Internet Safety.

All scholars 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 technological resources, scholars and employees must sign a statement indicating that they understand and will strictly comply with these requirements and acknowledging awareness that the school uses monitoring systems to monitor and detect inappropriate use of technological resources. 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.

1. **Rules for Use of School Technological Resources**
2. School 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 technological resources for commercial gain or profit is prohibited. Personal use of school technological resources for amusement or entertainment by scholars, faculty and staff 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 business, and is not otherwise prohibited by board policy or procedure.
3. Under no circumstance may software purchased by the school be copied for personal use.
4. Scholars 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 Scholar Conduct.
5. Users must follow any software, application, or subscription services terms and conditions of use.
6. 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.
7. Users must not circumvent fire walls. The use of anonymous proxies to circumvent content filtering is prohibited.
8. Users may not install or use any Internet-based file sharing program designed to facilitate sharing of copyrighted material.
9. Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).
10. Users must respect the privacy of others. When using e-mail, chat rooms, blogs, or other forms of electronic communication, scholars 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 scholars. For further information regarding what constitutes personal identifying information, see policy 4705/7825, Confidentiality of Personal Identifying Information. In addition, school employees must not disclose on school websites or web pages or elsewhere on the Internet any personally identifiable, private, or confidential information concerning scholars (including names, addresses, or pictures) without the written permission of a parent or guardian or an eligible scholar, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 4700, Scholar Records. Users also may not forward or post personal communications without the author’s prior consent.
11. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks, or data of any user connected to school 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.
12. Users may not create or introduce games, network communications programs, or any foreign program or software onto any school computer, electronic device, or network without the express permission of the technology director or designee.
13. 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.
14. Users are prohibited from using another individual’s ID or password for any technological resource without permission from the individual. Scholars must also have permission from the teacher or other school official.
15. Users may not read, alter, change, block, execute, or delete files or communications belonging to another user without the owner’s express prior permission.
16. Employees shall not use passwords or user IDs for any data system (e.g., the state scholar information and instructional improvement system applications, time-keeping software, etc.) for an unauthorized or improper purpose.
17. 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. Any user identified as a security risk will be denied access.
18. It is the user’s responsibility to back up data and other important files.
19. Teachers shall make reasonable efforts to supervise scholars’ use of the Internet during instructional time.
20. Views may be expressed on the Internet or other technological resources as representing the view of the school or part of the school only with prior approval by the executive director.

# Restricted Material on the Internet

The Internet and electronic communications offer fluid environments in which scholars may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to scholars. The board recognizes that it is impossible to predict with certainty what information on the Internet scholars may access or obtain. Nevertheless, school personnel shall take reasonable precautions to prevent scholars 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 executive director 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).

# 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 scholar may independently access the Internet, the scholar’s parent must be made aware of the possibility that the scholar could obtain access to inappropriate material while engaged in independent use of the Internet. The parent and scholar must consent to the scholar’s independent access to the Internet and to monitoring of the scholar’s Internet activity and e-mail communication by school personnel.

In addition, in accordance with the board’s goals and visions for technology, scholars may require accounts in third party systems for school related projects designed to assist scholars 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.

1. **Privacy**

Scholars, employees, visitors, and other users have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the school’s network, devices, Internet access, email system, or other technological resources owned or issued by the school, 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 technological resources or stored on servers or on the storage mediums of individual devices will be private.

The school 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 from liability, and complying with public records requests. School personnel shall monitor online activities of individuals who access the Internet via a school-owned device.

By using the school’s network, Internet access, email system, devices, or other technological resources, individuals consent to have that use monitored by authorized school personnel as described in this policy.

1. **Use of Personal Technology on School 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.  The principal may establish rules for as to whether and how personal technology devices (including, but not limited to smart phones, tablets, laptops, etc.) may be used on campus. Scholars’ devices are governed also by policy 4318, Use of Wireless Communication Devices. The school assumes no responsibility for personal technology devices brought to school.

1. **Personal Websites**

The executive director may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize the school name, logos, or trademarks without permission.

1. Scholars

Though school personnel generally do not monitor scholars’ Internet activity conducted on non-school devices during non-school hours, when the scholar’s online behavior has a direct and immediate effect on school safety or maintaining order and discipline in the school, the scholar may be disciplined in accordance with board policy (see the scholar behavior policies in the 4300 series).

1. Employees

Employees’ personal websites are subject to policy 7335, Employee Use of Social Media.

1. Volunteers

Volunteers are to maintain an appropriate relationship with scholars at all times. Volunteers are encouraged to block scholars from viewing personal information on volunteer personal websites or online networking profiles in order to prevent the possibility that scholars could view materials that are not age-appropriate. An individual volunteer’s relationship with the school may be terminated if the volunteer engages in inappropriate online interaction with scholars.

1. **Use Agreements**

All students, parents, and employees will be informed annually of the information in this policy.  Prior to using school’s technological resources, students and employees must agree to comply with the requirements of this policy and consent to the school’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 monitoring the student’s Internet activity and electronic mailbox issued by the school.

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

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 (policy 3227/7322), Scholar Behavior Policies (all policies in the 4300 series), Use of Wireless Communication Devices (policy 4313), Scholar 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: April 15, 2020

Revised: June 8, 2022