PARIS SPECIAL SCHOOL DISTRICT TECHNOLOGY RESPONSIBLE USE POLICY

Updated 2/11/20

The board provides its students and staff access to a variety of technology resources, including laptop computers and tablets. These resources provide opportunities to enhance learning and improve communication within the school community and with the larger global community. Through the school district'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 district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district 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

School district technological resources may only be used by students, staff and others expressly authorized by the Technological Department. The use of school district technological resources, including access to the Internet, is a privilege, not a right. Individual users of the school district's technological resources are responsible for their behavior and communications when using those resources. Responsible use of school district technological resources is use that is ethical, respectful, academically honest and supportive of school 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 code of ethics, including those prescribed in applicable board policies, the Student Handbook State and Federal Laws and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school district computers or electronic devices or who access the school network or the Internet using school district 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. Furthermore, all students must adhere to the PSSD Technology Use Guidelines as set forth in the Student Handbook. Prior to using the Internet, all students must be trained about appropriate on-line behavior as provided in policy 4.406 – Use of the Internet.

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 district 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 district 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 district technological resources for political purposes, sectarian religious purposes, or for commercial gain or profit is prohibited. Student personal use of school district technological resources for amusement or entertainment is 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 district business and is not otherwise prohibited by board policy or procedure.

2. School district technological resources are installed and maintained by members of the Technology Department. Students and employees shall not attempt to perform any installation or maintenance without the permission of the Technology Department.

3. Under no circumstance may software purchased by the school district be copied for personal use, unless otherwise permitted.

4. 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.

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. All users must comply with policy 5.500 – Discrimination/Harassment of Employees (Sexual, Racial, Ethnic, Religious) and 6.304 – Student Discrimination/ Harassment and Bullying/Intimidation when using school district technology.

6. The use of anonymous proxies to circumvent content filtering is prohibited.

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

8. Users may 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. For further information regarding what constitutes personal identifying information, see policy 4.406 – Use of the Internet. In addition, school employees must not disclose on school district 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 or a parent or guardian or an eligible student, except as

otherwise permitted by the Family Educational Rights and Privacy Act (FERPA) or policy 6.600 – 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 district technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance.

10. Users may not create or introduce games, network communications programs or any foreign program or software onto any school district computer, electronic device or network without the express permission of the Technology Department. Users enrolled in computer classes teaching network design or maintenance may, with the assistance of their instructor, create programs as required by the course curriculum.

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 for any technological resources without permission from the individual. We assigned laptops with an assigned password.

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

14. Employees shall not use PSSD email, password or user ID for personal use (for an unauthorized or improper purpose).

15. 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.

16. Teachers shall make reasonable efforts to supervise students' use of the Internet during instructional time, to ensure that such use is appropriate for the student's age and the circumstances and purpose of the use.

17. Views may be expressed on the Internet or other technological resources as representing the view of the school district or part of the school district only with prior approval by the superintendent or designee.

18. Without permission, users may not connect any personal technologies such as laptops and workstations, wireless access points and routers, etc. to a district owned and maintained local, wide or metro are network. For example, but not limited to: Mi-Fi, hotspots, Personal Digital Assistants, etc.

19. Connection of personal devices such as iPods, iPads, smartphones, PDAs, and printers are permitted but not supported by PSSD technical staff. Student teachers and other district invited guests can use the PSSD Guest network in support of their work inside PSSD 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).

20. Users must back up locally stored (i.e., not stored on the district network and/or Microsoft One Drive) data and other important files regularly. PSSD will at times perform maintenance on the equipment by imaging. All files not backed up to Microsoft One Drive will be deleted during this process. It is the responsibility of the user to ensure that locally synced files are syncing properly. Help Desk will assist any user with synchronization issues.

21. Those who use district owned and maintained technologies to access the Internet at home are responsible for both the cost and configuration of such use.

22. Employees and students who are issued district owned and maintained equipment must also follow these guidelines:

    a. Keep the equipment secure and damage free.

    b. Always use the provided protective laptop bag.

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

    d. Do not leave the equipment in your vehicle.

    e. Do not leave the equipment unattended.

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

    g. Do not allow pets near the equipment.

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

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

    j. Do not deface laptops or store anything extra in bags.

    k. Do not stack objects on top of the equipment.

    l. Do not leave the equipment outside.

    m. Do not use the equipment near water such as a pool.

    n. Do not check the equipment as luggage at the airport. It is usually advisable to carry any district owned equipment on board with you rather than checking it as luggage.

    o. Do not carry laptops by the display screen.

    p. Do not hang anything around or attach anything to the technology display panels such as lights, borders, etc. as this may hinder its performance.

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 district 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 4.406 – Internet Safety Measures, and responsible for 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 non-contracted services 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 accessed, downloaded, created or transmitted using school district technological resources or stored on services or data storage components of individual computers will be private. School district 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 district personnel shall monitor online activities of individuals who access the Internet via a school-owned computer.

Under certain circumstances, the board 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, as a response to a public records request or as evidence of illegal activity in a criminal investigation.

F. SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. Employees are responsible for reporting information of security violations to the help desk. Employees should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the district’s network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access.

Users of school district technology resources are expected to respect school district property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school district is responsible for any routine maintenance or standard repairs to school system computers.