SECTION I INSTRUCTION

IJNDB-R STUDENT DIGITAL DEVICES AND INTERNET USE AND SAFETY RULES

All students are responsible for their actions and activities involving school digital devices, tablets, printers, network and internet services, and for their computer files, passwords and accounts. The use of school digital devices, networks and other infrastructure by students is a privilege, not a right. These rules provide general guidance concerning the use of the school's digital devices and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity by students. Students, parents and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator or the Computer Systems Manager. These rules apply to all school digital devices (see definition for digital device in policy IJNDB) and all school-provided laptops wherever used, and all uses of school servers, internet access and networks regardless of how they are accessed.

A. Acceptable Use

1. The school's digital devices, printers, network and internet services are provided for educational purposes and research consistent with the school's educational mission, curriculum and instructional goals.

2. Students must comply with all Board policies, school rules and expectations concerning student conduct and communications when using school digital devices, printers, and network whether on or off school property.

3. Students also must comply with all specific instructions from school staff and volunteers when using the school's digital devices and must read and sign an acceptable use policy.

B. Prohibited Uses

Unacceptable uses of school digital devices include, but are not limited to, the following:

1. **Accessing or Communicating Inappropriate Materials –** Students may not access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/or illegal materials or messages.

2. **Illegal Activities and Digital Citizenship –** Students must practice good digital citizenship and may not use the school's digital devices, network and internet services for any illegal activity or in violation of any Board policy/procedure or school rules. The school assumes no responsibility for illegal activities of students while using school digital devices.

3. **Violating Copyrights or Software Licenses –** Students may not copy, download or share any type of copyrighted materials (including music or films) without the owner's permission; or copy or download software without the express authorization of the

Computer Systems Manager. Unauthorized copying of software or other copyrighted material such as movies, etc. is illegal and may subject the copier to substantial civil and criminal penalties. The school assumes no responsibility for copyright or licensing violations by students.

4. **Plagiarism –** Students may not represent as their own work any materials obtained on the internet (such as term papers, articles, music, etc). When internet sources are used in student work, the author, publisher and web site must be identified.

5. **Use for Non-School-Related Purposes -** Using the school's digital devices, tablets, printers, network and internet services for any personal reasons not connected with the educational program, authorized after-school activities or school assignments.

6. **Misuse of Passwords/Unauthorized Access –** Students may not share passwords; use other users' passwords; access or use other users' accounts; or attempt to circumvent network security systems.

7. **Malicious Use/Vandalism –** Students may not engage in any malicious use, disruption or harm to the school's digital devices, printers, network and internet services, including but not limited to hacking activities and creation/uploading of computer viruses. Students shall take every precaution to ensure that the digital devices are protected and safe from damage, including liquid spills, drops, etc.

8. **Avoiding School Filters –** Students may not attempt to or use any software, utilities, proxy servers, peer-to-peer networks or other means to access internet sites or content blocked by the school filters. Students may not bypass school networks by broadcasting a personal network device from a cell phone or other personal device.

9. **Unauthorized Access to Blogs/Social Networking Sites, Etc. –**Students may not access blogs, social networking sites, etc. to which student access is prohibited by filters or other means. Occasionally access to such sites or tools may be permissible when authorized by a teacher or administrator for educational purposes.

10. **Mass Email –** Students must not send mass email or SPAM from a school digital device or network.

11. **Inventory Asset Tags -** Students are not permitted to remove or deface asset tags from digital devices.

C. Compensation for Losses, Costs and/or Damages

The student and his/her parents are responsible for compensating the school for any losses, costs or damages incurred for violations of Board policies/procures and school rules while the student is using school digital devices or network, including the cost of investigating such violations. The school assumes no responsibility for any unauthorized charges or costs incurred by a student while using school digital devices or network.

D. Student Security

A student is not allowed to reveal his/her full name, address, telephone number, social security number or other personal information on the internet while using a school digital device without prior permission from a teacher. Students should never agree to meet people they have contacted through the internet without parental permission. Students should inform their teacher if they access information or messages that are dangerous, inappropriate or make them uncomfortable in any way.

E. System Security

The security of the school's digital devices, network and internet services is a high priority. Any student who identifies a security problem must notify his/her teacher or building administrator immediately. The student shall not demonstrate the problem to others or access unauthorized material.

F. Additional Rules for Use of Privately-Owned Digital Devices by Students

1. A student's privately-owned digital device, smart phone, tablet etc. in school must adhere to all Student Digital Devices Use Policies and Rules and the Acceptable Use Policy. There must be an educational basis for the use of any digital device brought from home.

2. The Computer Systems Manager or staff will determine whether a student's privately-owned digital device meets the school's network requirements and will determine if that device may be used in the school buildings.

3. Use of these devices may be prohibited if it is determined that there is not a suitable educational basis and/or if the demands on the school's network or staff would be unreasonable.

4. The student is responsible for proper care and security of his/her privately-owned digital device, including any costs of repair, replacement or any modifications needed to use the digital device at school.

5. The school is not responsible for damage, loss or theft of any privately-owned devices.

6. Students are required to comply with all Board policies, administrative procedures and school rules while using privately-owned digital devices at school.

7. Students have no expectation of privacy in their use of a privately-owned digital device while at school. The school reserves the right to search a student's privately-owned device if there is reasonable suspicion that the student has violated Board policies, administrative procedures or school rules, or engaged in other misconduct while using the device.

.

8. Violation of any Board policies, administrative procedures or school rules involving a student's privately-owned digital device may result in the revocation of the privilege of using the device at school and/or disciplinary action.

9. The school may confiscate any privately-owned digital device used by a student in school

without authorization as required by these rules. The contents of the device may be searched in accordance with applicable laws and policies.

Cross Reference: IJNDB – Student Digital Devices and Internet Use and Safety

First Reading: 5/25/11, 6/27/18
Adopted: 6/22/11, 8/22/18
Revised: 2/29/12
Reviewed: 5/23/18