STUDENT COMPUTER/ DEVICE AND INTERNET USE RULES

These rules accompany Board policy IJNDB (Student Computer/device and Internet Use). All students are responsible for their actions and activities involving school unit computers/devices, networks, and Internet services, and for their computer/device files, passwords, and accounts.

These rules provide general guidance concerning the use of the school unit's computers/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 the Building Principal.

A. **Acceptable Use**

1. The school unit's computers/devices, networks, and Internet services are provided for educational purposes and research consistent with the school unit's educational mission, curriculum, and instructional goals.

2. Students must comply with all board policies, school rules, and expectations concerning student conduct and communications apply when students are using computers/devices, whether the use is on or off school property.

3. Students also must comply with all specific instructions from school administrators, school staff or volunteers when using the school unit's computers/devices.

B. **Prohibited Uses**

Unacceptable uses of school unit computers/devices that are expressly prohibited 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/cyberbullying and/or illegal materials or messages.

2. **Illegal Activities** – Students may not use the school unit's computers/devices, network and Internet services for any illegal activity or in violation of any Board policy/procedure or school rules. The school unit assumes no responsibility for illegal activities of students while using school computers/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 Technology Coordinator.

Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for copyright or licensing violations by students. See Board policy/procedure EGAD – Copyright Compliance.

4. **Plagiarism** – Students may not represent as their own work any material 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. **Misuse of Passwords/Unauthorized Access** – Students may not share passwords (except with authorized school employees); use other users' passwords; access or use other users' accounts; or attempt to circumvent network security systems.

6. **Malicious Use/Vandalism** – Students may not engage in any malicious use, disruption or harm to the school unit's computers/devices, network and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

7. **Avoiding School Filters** – Students may not attempt to or use any software, utilities or other means to access Internet sites or content blocked by the school filters. If a student believes filtering should be less restrictive on a temporary basis for specific, bona fide research purposes he/she should discuss the matter with his/her teacher.

8. **Authorized/Unauthorized Access to Blogs/Social Networking Sites, Etc.** There is an overabundance of blogs, social networks, and other web sites that are too numerous to name or regulate. However, students and teachers are expected to access and utilize blogs, social networks, and web sites that are compatible with the school code of conduct and behavioral norms. Teachers and administrators are to provide guidance and direction to students on the use of an access to blogs, social networks, and other web sites.

C. **Consequences for Violation of Computer/Device Use Policy and Rules**

1. Compliance with the school unit's policies and rules concerning computer/device use is mandatory. Students who violate these policies and rules may, after having been given the opportunity to respond to an alleged violation, have their computer/device privileges limited, suspended, or revoked. Such violations may also result in disciplinary action, referral to law enforcement, and or legal action.

2. The Building Administrator shall have final authority to decide whether a student's privileges will be limited, suspended or revoked based upon the circumstances of the particular case, the student's prior disciplinary record, and any other relevant factors.

3. The Building Administrator can require student(s) to attend the per-use informational meeting.

D. **No Expectation of Privacy**

RSU 56 computers/devices remain under the control, custody, and supervision of the school unit at all times. Students have no expectation of privacy in their use of school computers/devices including email, stored files, and Internet access logs.

E. **Compensation for Losses, Costs, and/or Damages**

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

F. **Student Security**

A student is not allowed to reveal his/her full name, address or telephone number, photograph or any other personal information on the Internet without prior permission from their parent/guardian and teacher. At no time should a student reveal their social security number. 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.

G. **System Security**

The security of the school unit's computers/devices networks, and Internet services is a high priority. Any student who identifies a security problem must notify his/her teacher immediately. The student shall not demonstrate the problem to others or access unauthorized material. Any user who attempts to breach system security, causes a breach of system security, or fails to report a system security problem shall be subject to disciplinary and/or legal action in addition to having his/her computer/device privileges limited, suspended, or revoked.

H. **Additional Rules for Devices Issued to Students**

1. Devices/iPads are loaned to students as an educational tool and may be used for purposes specifically authorized by school employees and the MLTI program.

2. Parent(s)/guardian(s) and student(s) are required to attend a pre-use informational meeting designed by the Building Administrator before a device will be issued to their child. The meeting will orient parents on the

expectations for care of school-issued devices, Internet safety, and the school unit's rules in regard to use of this technology. Before a device is issued annually to a student, the student and the parent/guardian must sign the school's "student device acceptable use" form.

3. Students and their parents are responsible for the proper care of devices at all times, whether on or off school property, including costs associated with repairing or replacing the device. RSU 56 offers a device protection plan for parents to cover replacement costs and/or repair costs for damages not covered by the device warranty. Parents who choose not to enroll in the device protection plan should be aware that they are responsible for any costs associated with loss, theft, or damage to a device issued to their child.

4. Loss, theft, or damage or accessories of a device must be reported immediately to principal/vice principal, and, if stolen, to the local law enforcement authority as well.

5. The Board's policy and rules concerning computer/device and Internet use apply to use of devices at any time or place, on or off school property. Students and parent(s)/guardian(s) are responsible for obeying any additional rules concerning care of devices issued by school staff.

6. Violation of policies or rules governing the use of computer/device or any careless use of a device may result in a student's device being confiscated and/or a student only being allowed to use the device under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies or school rules.

7. Parents may be informed of their child's login password. Parents are responsible for supervising their child's use of the device and Internet access when in use at home.

8. The device may only be used by the student to whom it is assigned and by family members, to the extent permitted by Maine's device program.

9. All use of school-loaned devices by all persons must comply with the school's Student Computer/Device and Internet Use Rules.

10. Devices must be returned in acceptable working order at the end of the school year or whenever requested by school staff.

Cross Reference: EGAD – Copyright Compliance
IJNDB – Student Computer/device and Internet Use
IJNDB-E – Student Computer/device Internet Acceptable Use Form

Adopted: July 11, 2017