# Student Digital Device and Internet Use and Internet Safety Procedure

Each student is responsible for his/her actions and activities involving RSU 40/MSAD 40 (District) digital devices, networks and Internet services, and for their computer files, passwords and accounts. These regulations provide general guidance concerning the use of the District's digital devices and examples of prohibited uses; however, they do not attempt to describe every possible prohibited activity. Students, parents and school staff who have questions about whether a particular activity is prohibited are encouraged to contact a building administrator or the Technology Coordinator. These regulations apply to all school digital devices wherever used, and all uses of school servers, Internet access and networks regardless of how they are accessed.

**Consequences for Violation**
Student use of the District's digital devices, networks and Internet services is a privilege, not a right. Compliance with the District's policies and regulations on Student Digital Device and Internet Use and Internet Safety is mandatory. Students who violate these policies and regulations may have their device privileges limited, suspended or revoked. Such violations may also result in disciplinary action, referral to law enforcement and/or legal action.

The Superintendent/designee shall have the final authority to decide whether a student's privileges will be limited, suspended or revoked.

**Acceptable Use**
The District's digital devices, networks and Internet services are provided for educational purposes and research consistent with the District's educational mission, curriculum and instructional goals.

All Board policies, school regulations and expectations concerning student conduct and communications apply when students are using digital devices, whether on or off school property.

Students are also expected to comply with all specific instructions from teachers and other school staff when using the District's digital devices.

**Prohibited Uses**

Examples of unacceptable uses of District digital devices that are prohibited include, but are not limited to, the following:

1. Accessing Inappropriate Materials -Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing, bullying and/or illegal materials or messages.

2. Illegal Activities -Using the District's digital devices, networks and Internet services for any illegal activity or in violation of any Board policy or school regulations. The District assumes no responsibility for illegal activities of students while using school digital devices.

3. Violating Copyrights – Copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission (see Board policy/procedure EGAD – Copyright Compliance). The District assumes no responsibility for copyright violations by students.

4. Copying Software -Copying or downloading 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 District assumes no responsibility for illegal software copying by students.

5. Plagiarism -Representing as one's 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.

6. Non-School-Related Uses -Using the District's digital devices, networks and Internet services for non-school related purposes as defined by the school administration.

7. Misuse of Passwords/Unauthorized Access -Sharing passwords, using other users' passwords, and accessing or using other users' accounts or attempt to circumvent network security systems.

8. Malicious Use/Vandalism -Any malicious use, disruption or harm to the District's digital devices, networks and Internet services, including but not limited to hacking activities and creating/uploading of computer viruses.

9. Unauthorized Access to Blogs/Social Networking Sites, etc. -Accessing blogs, social networking sites, etc. that are not approved for educational purposes or without specific authorization from a school administrator.

10. Avoiding School Filters – Students may not attempt to or use any software, utilities or other means to access Internet sites or content blocked by school filters.

11. Use of Recording Devices - The use of recording devices, such as cameras, is strictly prohibited in locker rooms and restrooms. In all other locations, students are required to obtain permission from a supervising teacher or school administrator before using a recording device to capture any individual either audibly and/or visually.

**No Expectation of Privacy**
In the use of the District's digital devices, networks, and Internet services, students shall have no expectation of privacy, including e-mail, stored files and Internet access logs.

**Compensation for Losses, Costs and/or Damages**
Students and their parents are responsible for compensating the District for any losses, costs or damages incurred by the District for violations of Board policies and school regulations while the student is using District digital devices, including the cost of investigating such violations. The District assumes no responsibility for any unauthorized charges or costs incurred by a student while using District digital devices.

**Student Security**
A student is not allowed to reveal their full name, address, telephone number, social security number or other personal information on the Internet 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.

**System Security**
The security of the District's digital devices, networks and Internet services is a high priority. Any student who identifies a security problem must notify their 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 their computer privileges being suspended or revoked.

## Additional Regulations for Use of Privately-Owned Digital Devices by Students

1. A student who wishes to use a privately-owned digital and/or cellular device, which will access the school network, must complete a Student Request to Use Privately-Owned Device form. The form must be signed by the student, their parent, a sponsoring teacher, the school principal and the Technology Coordinator. There must be an educational basis for any request.

2. The Technology Coordinator will determine whether a student's privately-owned digital device meets the District's network requirements.

3. Requests may be denied if it is determined that there is not a suitable educational basis for the request and/or if the demands on the District's network or staff would be unreasonable.

4. The student is responsible for proper care of their privately-owned computer, including any costs of repair, replacement or any modifications needed to use the computer at school.

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

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

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

8. Violation of any Board policies, administrative procedures or school regulations 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 District may confiscate any privately-owned digital device used by a student in school without authorization as required by these regulations. The contents of the device may be searched in accordance with applicable laws and policies.

**Use of First Class/Email**

1. Students in grades 7-12 may be provided email access. When a student leaves the district, their access will be removed within 30-60 days. Email accounts inactive for120 days will be deleted systematically.

2. FIRST CLASS Record Retention: Email messages will be systematically deleted 160 days from the originating date. Exception: conferences are set by default to expire in 60 days but may be adjusted. An archiving system is in place for long-term storage of messages. With the approval of the Superintendent, the technology team will determine the expiration time line.

**Additional Regulations for Digital Devices Issued to Students**

1. Digital devices are issued to students as an educational tool and may be used for purposes specifically authorized by school staff and the MLTI program. Violation of policies, regulations, or procedures governing the use of technology may result in a student's digital device being confiscated or otherwise restricted. Students will be subjected to disciplinary action for any violations of policies, procedures or regulations.

2. Students are required to demonstrate acceptable use of technology and standards for digital citizenship and sign an acknowledgement form.

3. Students and families are responsible for the proper care of digital devices at all times, whether on or off of school property, and may be responsible for any costs associated with repairing or replacing of the digital device and accessories that are not covered by the digital device warranty.

4. If a digital device is lost or stolen, this must be reported to the school principal and technology director immediately. If a digital device is stolen, a report should be made to the local police and school principal immediately.

5. The Board's policy and regulation concerning digital devices and Internet use apply to use of digital devices at any time or place, on or off school property. Students are responsible for obeying any additional regulation concerning care of digital devices issued by school staff.

6. Parents will be informed of their student's login password. Parents are responsible for supervising their student's use of the digital device and Internet access when in use at home.

7. The digital device may only be used by the student to whom it is assigned and the supervising parent/guardian who also must comply with the school's Student Digital Device and Internet use and Internet Safety policy and regulations.

8. Digital devices must be returned in acceptable working order at the end of the school year, or whenever requested by school staff.

9. Digital devices may not be taken in locker rooms, on playing fields, courts, etc. Arrangements with parents for digital device pick-ups must be made in advance for students participating in extra-curricular activities.

Reference: Policy IJNDB

*This is a required policy.*

Adopted: October 2, 2008

Revised: September 15, 2011
October 15, 2015