Student Technology And Internet Use Rules

These rules accompany Board policy IJNDB (Student Technology and Internet Use and Internet Safety). Each student is responsible for his/her actions and activities involving district technology (including I-Pads, tablets, laptops and other devices issued to students), networks, and Internet services, and for his/her computer files, passwords, and accounts.

These rules provide general guidance concerning the use of the school unit issued technology (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 or the Director of Technology.

A. Acceptable Use

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

All Board policies, school rules, and expectations concerning student conduct and communications apply when students are using district issued devices, whether the use is on or off school property.

Students are also expected to comply with all specific instructions from school administrators, school staff or volunteers when using the district's devices.

B. Consequences for Violation of the District Technology Use Policy and Rules

Student use of the district technology, networks and internet services are a privilege, not a right. Compliance with the school unit's policies and rules concerning district 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 technology privileges limited, suspended, or revoked. Such violations may also result in disciplinary action, referral to law enforcement, and or legal action.

The building principal 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.

C. Prohibited Uses

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

1. **Accessing or Posting Inappropriate Materials** – Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal materials or engaging in "cyber bullying;"

2. **Illegal Activities** – Using the district's devices, networks, and Internet services for any illegal activity or in violation of any Board policy or school rules. The school unit assumes no responsibility for illegal activities of students while using school technology.

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 school unit assumes no responsibility for copyright violations by students;

4. **Copying Software** – Copying or downloading software without the express authorization of the Director of Technology. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school unit 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 website must be identified;

6. **Non-School-Related Uses** – Using the district's technology/devices, networks, and Internet services for non-school related purposes such as private financial gain; commercial , advertising or solicitation purposes; or any other personal use not connected with the educational program or assignments;

7. **Misuse of Passwords/Unauthorized Access** – Sharing passwords, using other users' passwords, and accessing or using other users' accounts; or attempting to circumvent network or computer security systems.

8. **Malicious Use/Vandalism** – Any malicious use, disruption or harm to the district's technology/devices, networks, and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.

9. **Avoiding School Filters** – Attempting to or using any software, utilities or other means to access Internet sites or content blocked by school filters.

10. **Unauthorized Access to Blogs/Chat Rooms/Social Networking Sites/Gaming Sites –** Accessing blogs, chat rooms, social networking sites and gaming sites etc. to which student access is prohibited. Such sites may only be used under the direct supervision of a supervising teacher.

D. **No Expectation of Privacy**

RSU 9's technology/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 district technology/devices, including email, stored files, and Internet access logs.

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

The student and their 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 school rules while the student is using district technology/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 district technology, including, but not limited to credit card charges, long distance telephone charges, equipment and line costs, or any illegal use of its computers, such as copyright violations.

F. **Student Security**

A student is not allowed to reveal his/her full name, address or 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.

G. **System Security**

The security of the district's technology, 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 privileges limited, suspended, or revoked.

H. **Additional Rules for District Technology Issued to Students**

1. Technology/devices are loaned to students as an educational tool and are only authorized for use in completing school assignments.

2. Before any district technology/device is issued to a student, the student and their parent must sign the school's "acceptable use" agreement. Parents are required to either attend an informational meeting and/or sign a permission slip before any district technology will be issued to their child. The meeting or permission slip will orient parents to the goals and workings of the district technology program, expectations for care of school-issued devices, Internet safety, and the school unit's rules in regard to use of this technology.

3. Students and their parents are responsible for the proper care of district technology/ devices at all times, whether on or off school property, and may be responsible for malicious or intentional damage, including costs associated with repairing or replacing the loaned technology/device issued to their child.

4. Loss or theft of a loaned device must be reported immediately to building administration immediately. If the device is stolen, a report should be made to the local police and Director of Technology immediately.

5. The Board's policy and rules concerning district technology/devices and Internet use apply to use of loaned devices at any time or place, on or off school property. Students 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 district technology, 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 devices under the direct supervision of school staff. The student will also be subject to disciplinary action for any Board policies or school rules.

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

8. Technology/devices may only be used by the student to whom it is assigned and by family members, to the extent permitted by the MLTI program. Any family member using the device must abide by all school board policies and school rules.

9. Technology/devices must be returned in acceptable working order at the end of the school year or whenever requested by school staff.

I. Use of Privately-Owned Computers by Students

1. A student who wishes to use a privately-owned device in school must make a request in writing to the Director of Technology and building principal. The request must be signed by both the student and a parent or guardian.

2. The Director of Technology will determine whether the student's privately-owned device meets the school unit'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 of the school unit's network or staff would make it unreasonable.

Cross Reference: EGAD – Copyright Compliance
IJNDB – Student Computer and Internet Use