

STUDENT COMPUTER AND INTERNET USE RULES

These rules implement Board policy IJNDB – Student Computer and Internet Use. The rules are intended to provide general guidelines and examples of prohibited uses but do not attempt to state all required or prohibited activities by users. Students, parents, and school staff who have questions regarding activities that may be prohibited are asked to contact a building administrator or the Technology Director.

A. Computer Use is a Privilege, Not a Right

Student use of the school unit’s computers, electronic devices, networks, Internet and other services is a privilege, not a right. Unacceptable use/activity may result in suspension or cancellation of privileges as well as additional disciplinary and/or legal action. The building principal shall have final authority to decide whether a student’s privileges will be denied or revoked.

B. Acceptable Use

Student access to the school unit’s computers, networks, Internet and other services are provided for educational purposes consistent with the school unit’s educational mission, curriculum and instructional goals.

The same rules and expectations govern student use of computers as apply to other student conduct and communications.

Students are further expected to comply with these rules and all specific instructions from the teacher or other supervising staff member/volunteer when accessing the school unit’s computers, networks, Internet and other services.

Students’ use of computers and resources is limited to educational purposes, regardless of the location of the student or the computer.

C. Prohibited Use

The user is responsible for his/her actions and activities involving school unit computers, networks, Internet and other services and for his/her computer files, passwords and accounts. Examples of unacceptable uses that are expressly prohibited include but are not limited to the following:

1. **Accessing Inappropriate Materials** – Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal;
2. **Illegal Activities** – Using the school unit’s computers, networks, Internet and other services for any illegal activity or activity that violates other Board policies, procedures and/or school rules;

3. **Violating Copyrights** – Copying, downloading, uploading, or sharing copyrighted materials without the owner’s permission;
4. **Plagiarism** – Representing as one’s own work any materials obtained on the Internet (such as term papers, articles, etc.). When Internet sources are used in student work, the author, publisher and Website must be identified;
5. **Copying Software** – Copying or downloading software without the express authorization of the system administrator or teacher;
6. **Non-School-Related Uses** – Using the school unit’s computers, networks, Internet and other services for non-school-related purposes such as private financial gain, commercial, advertising or solicitation purposes;
7. **Misuse of Passwords/Unauthorized Access** – Sharing passwords, using other users’ passwords and/or accessing other users’ accounts;
8. **Malicious Use/Vandalism** – Any malicious use, disruption or harm to the school unit’s computers, networks, Internet and other services, including but not limited to hacking activities and creation/uploading of computer viruses;
9. **Filters** – Over riding, or disabling district filters by anyone other than the District’s authorized designee.

D. **No Expectation of Privacy**

RSU 19 retains control, custody and supervision of all computers, networks and Internet services owned or leased by the school unit. The school unit reserves the right to monitor all computers, Internet, networks and other activity by students. Students have no expectations of privacy in their use of school computers, including e-mail and stored files.

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

The student and/or the student’s parent/guardian shall be responsible for compensating the school unit for any losses, costs or damages incurred by the school unit related to violations of policy IJNDB and/or these rules, including investigation of violations.

F. **School Unit Assumes No Responsibility for Unauthorized Charges, Costs or Illegal Use**

The school unit assumes no responsibility for any unauthorized charges made by students including but not limited to credit card charges, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

G. **Student Security**

A student shall not reveal his/her full name, address or telephone number on the Internet without prior permission from a supervising teacher. Students will not post pictures, either their own or pictures of others, without proper permission. Students should never meet people they have contacted through the Internet without parental permission. Students should inform their supervising teacher if

they access information or messages that are dangerous, inappropriate or make them uncomfortable in any way.

H. **System Security**

The security of the school unit's computers, networks, Internet and other services is a high priority. Any user who identifies a security problem must notify an administrator. The user shall not demonstrate the problem to others. Any user who attempts or causes a breach of system security shall have his/her privileges revoked and may be subject to additional disciplinary and/or legal action.

I. **Parental Permission Required**

Students and their parent/guardian are required to sign and return the Computer/Internet Access Acknowledgment Form (IJNDB-E) before being allowed to use school computers.