

STUDENT COMPUTER AND INTERNET USE RULES

Each student is responsible for his/her actions and activities involving school district computers and laptops, networks and Internet services, and for his/her computer files, passwords and accounts. These rules provide general guidance concerning the use of district computers and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity. Students, parents and school staff who have questions about whether a particular activity or use is prohibited are encouraged to contact a building administrator or the Technology Director.

A. Consequences for Violation of Computer Use Policy and Rules

Student use of the district computers, networks and Internet services is a privilege, not a right. Compliance with the district’s policies and rules concerning computer use is mandatory. Students who violate these policies and rules may have their computer 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 the 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 pertinent factors.

B. Acceptable Use

The district’s computers, 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, district rules and expectations concerning student conduct and communications apply when students are using computers. Students are also expected to comply with all specific instructions from teachers and other school staff or volunteers when using the district’s computers.

C. Prohibited Uses

Examples of unacceptable uses of district computers 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 defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal materials.
2. Illegal Activities: Using the district’s computers, networks and Internet services for any illegal activity or in violation of any Board policy or school rules, including bullying or harassing behavior toward students or other persons. The district assumes no responsibility for illegal activities of students while using school computers.

SANBORN REGIONAL SCHOOL DISTRICT

SRSD File: JICL-R

3. **Violating Copyrights:** Copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission. The district assumes no responsibility for copyright violations by students
4. **Copying Software:** Copying or downloading software without the express authorization of the Technology Director. 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 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
6. **Non-School Related Uses:** Using the district's computers, 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.
8. **Malicious Use/Vandalism:** Any malicious use, disruption or harm to the district's computers, networks and Internet services, including but not limited to hacking activities and creation/ uploading of computer viruses.
9. **Unauthorized Access to Blogs/Chat Rooms/Social Networking Sites:** Accessing blogs, chat rooms or social networking sites without specific authorization from the supervising teacher.

D. No Expectation of Privacy

The Sanborn Regional School District's computers remain under the control, custody and supervision of the school district at all times. Students have no expectation of privacy in their use of district computers, including e-mail, stored files and Internet access logs.

E. Compensation for Losses, Costs and/or Damages

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

F. 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 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 school district's computers, 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 subjected to disciplinary and/or legal action in addition to having his/her computer privileges limited, suspended or revoked.

H: Additional Rules for Use of Personally-Owned Computers by Students

1. A student who wishes to use a personally-owned computer in school must complete a Student Personal Computer/Other Electronic Device Registration and Agreement form. The form must be signed by the student, his/her parent, a sponsoring teacher, the school principal and the Director of Technology. There must be a legitimate educational basis for any request.
2. The Director or Technology will determine whether a student's personally-owned computer meets the district's requirements.
3. Requests may be denied if it is determined that there is not a legitimate 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 his/her personally-owned computer, including any costs of repair, replacement or any modifications needed (including installation of up-to-date anti-virus software) to use the computer at school.
5. The district is not responsible for damage, loss or theft of any personally-owned computer.
6. Students are required to comply with all Board policies, administrative procedures and school rules while using personally-owned computers at school. Students are not allowed to access the district's network without specific authorization from a school administrator.

SANBORN REGIONAL SCHOOL DISTRICT

SRSD File: JICL-R

7. Students have no expectation of privacy in their use of a personally-owned computer while at school. The district reserves the right to search a student's personally-owned computer 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 computer.
8. Violation of any Board policies, administrative procedures or school rules involving a student's personally-owned computer may result in the revocation of the privilege of using the computer at school and/or disciplinary action.
9. The district may confiscate any personally-owned computer used by a student in school without authorization as required by these rules.

Related Policies: GBEF - Staff and Volunteer Access to Networks and Internet

Original Effective: September 18, 1996

Revised: November 28, 2001

Formally IJKB-R

Revised: August 11, 2010

Reaffirm: October 5, 2011