NEPN/NSBA Code: IJNDB-R

STUDENT COMPUTER AND INTERNET USE RULES

These rules implement Board policy IJNDB – Student Computer and Internet Use. All students are responsible for their actions and activities involving school unit computers, electronic devices, network, and Internet services, and for their computer files, passwords and accounts. 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. Failure to comply with Board policy IJNDB and these rules may result in loss of computer and Internet access privileges, disciplinary action, and/or legal action.

A. Computer Use is a Privilege, Not a Right - Student use of the school unit's computers, electronic devices (including personally owned devices used at school), networks, school provided accounts, 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/technology director or other designee 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, electronic devices, 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 electronic devices, networks, and accounts as apply to other student conduct and communications no matter where the devices and accounts are used.

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

1. Accessing or Communicating 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, bullying/cyberbullying and/or illegal materials or messages;

2. Illegal Activities – Using the school unit's computers, electronic devices, networks, Internet and other services for any illegal activity or activity that violates other any Board policies, procedures and/or school rules. SAD #4 assumes no responsibility for illegal activities of the students while using school computers, electronic devices, account, or networks;

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. SAD #4 assumes no responsibility for copyright or licensing violations by students; (See Board policy/procedure EGAD – Copyright Compliance)

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. 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;

6. Misuse of Passwords/Unauthorized Access –Students may not share passwords (except with authorized school employees), use other users' passwords and/or access other users' accounts, or attempt to circumvent network security systems;

7. Malicious Use/Vandalism – Any malicious use, disruption or harm to the school unit's computers, electronic devices, networks, Internet and other services, including but not limited to hacking activities and creation/uploading of computer viruses;

8. 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 or contact the Technology Director.

9. Unauthorized access to blogs/social networking sites, etc. – Students may not access blogs, social networking sites, etc. to which student access is prohibited by the school's filter.

D. No Expectation of Privacy - The school unit retains control, custody and supervision of all computers, electronic devices, networks and Internet services owned or leased by the school unit. The school unit reserves the right to monitor all computers, electronic devices, Internet, networks and other activity by students. Students have no expectations of privacy in their use of school computers, electronic devices, school accounts, including e-mail and stored files or personal devices used in the school.

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 board policies/procedures and/or these rules, including the cost of 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, social security number or other personal information on the Internet without prior permission from a supervising teacher. The use of cameras or the camera/video function on any devices is strictly prohibited in the locker rooms and bathrooms. Students will not post pictures or videos online, 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.

System Security - The security of the school unit's computers, electronic devices, 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.

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

Cross Reference: IJNDB – Student Computer and Internet Use

Adopted: May 9, 2000

Revised: December 9, 2003
November 14, 2006
November 9, 2010
May 11, 2015