NEPN/NSBA Code: IJNDB

# MILLINOCKET SCHOOL BOARD POLICY
# STUDENT COMPUTER, INTERNET AND ELECTRONIC DEVICE USE AND CYBER SAFETY

The school unit provides computers, networks and Internet access to support the opportunities for students and school staff. The Board believes that the resources available through the Internet are of significant value in the learning process and preparing students for future success. At the same time, the unregulated availability of information and communication on the Internet requires that schools establish reasonable controls for lawful, efficient and appropriate use of this and other technology.

Student use of school computers, networks, Internet services and other electronic devices is a privilege not a right. Students are required to comply with this policy, the accompanying rules (IJNDB-R) and any other acceptable use or similar policies and procedures that may be adopted at the building or district level. Students who violate the policy, its regulations, supplemental policies or procedures, and/or rules may have their computer or other electronic device privileges revoked and may also be subject to further disciplinary and/or legal action.

All school unit computers remain under the control, custody and supervision of the school unit. The school unit reserves the right to monitor all student computer and Internet activity. Students have no expectation of privacy in their use of computers at school.

Student laptop computers are generally intended for in-school use. Computer laptop procedures and rules will be adopted for home use and will include clearly defined provisions for: insuring the equipment, permission forms, expectations for appropriate use, and orientation sessions for parents and students.

While reasonable precautions will be taken to supervise student use of the Internet and other electronic devices, the school unit cannot reasonably prevent all inappropriate uses, including access to objectionable materials and communication with persons outside of the school, in violation of Board policies/procedures and school rules. The school unit is not responsible for the accuracy or quality of information that students obtain through the Internet.

Before a student is allowed to use school computers and Internet services, the student and the student's parent/guardian must sign and return the

Computer/Internet Access Acknowledgment (IJNDB-E) to the school each year. The signed acknowledgment will be retained by the school.
Students and parents shall be informed of this policy/procedure on an annual basis through handbooks and/or other means selected by the Superintendent.

The Superintendent shall be responsible for overseeing the implementation of this policy and the accompanying rules and for advising the Board of the need for any future amendments or revisions to the policy/rules. The administration may also develop additional administrative procedures/rules governing the day-to-day management and operations of the school unit's computer, internet and any other electronic devices used on the school premises, as long as they are consistent with the Board's policy/rules. The Superintendent may delegate specific responsibilities to building principals and others as deemed appropriate.

## CYBER SAFETY

The Millinocket School Department uses filtering technology designed to block materials that are obscene or harmful to minors and child pornography. Although the Millinocket School Department takes precautions to supervise student use of the internet, parents should be aware that the Millinocket School Department cannot reasonably prevent all instances of inappropriate computer and internet use by student in violation of Board policies and rules, including access to objectionable materials and communication with persons outside of the school. The Millinocket School Department is not responsible for the accuracy or quality of information that students obtain through the internet.

In the interest of student safety ("cyber safety"), The Millinocket School Department also educates students about on-line behavior, including interacting on social networking sites and chat rooms, and issues surrounding cyberbullying awareness and response.

The Superintendent is responsible for implementing this policy and accompanying "acceptable use" rules and for documenting student internet safety training. The Superintendent/designee may implement additional administrative procedures or school rules consistent with Board policy to govern the day to day management and operations of the school's computer system.

Students and parents shall be informed of this policy and the accompanying rules through student handbooks, the school website, and/or means selected by the Superintendent.

Cross Reference: GCSA – Employee Computer, Internet and Electronic Device Use

# IJNDB-R –Student Computer, Internet, and Electronic Devise Use Rules

Original: 03-19-97
1st Reading: 01-02-07
2nd Reading and Adoption to Replace Original: 02-13-07
Amended: 1-11-12
First Reading: 1-31-12
Adopted: 2-28-12
Reviewed: 3-8-16 (No changes)

NEPN/NSBA Code: IJNDB-R

# MILLINOCKET SCHOOL BOARD POLICY
# STUDENT COMPUTER, INTERNET AND ELECTRONIC DEVICE USE RULES

The school unit has access to the world through the Internet, an electronic highway connection of thousands of computers and millions of individual users. Our connections will allow students, teachers, and staff to gather information and interact with people all over the world. The Internet offers vast, diverse, and unique resources. By providing staff and students' access, we promote educational excellence through resource sharing, innovation, and communication. The Internet exposes users to a wide variety of cultures. Such exposure is usually an asset, but may occasionally provide ideas and opinions that are not the norm for our area. To counter this potential drawback, we are monitoring student internet activity and continue to filter categories that may be offensive. Even with these precautions, however, we can not filter every piece of electronic mail or every file found on a computer linked to the Internet. Students will be instructed to avoid inappropriate activities and will be disciplined if found in violation of these rules.

These rules implement Board policy IJNDB – Student Computer, Internet and Electronic Device 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. 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, networks internet services and other electronic devices 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 and Guidelines

Student access to the school unit's computers, networks and Internet services are provided for educational purposes and research

consistent with the school unit's educational mission, curriculum and instructional goals.

Access to the school unit's computers, networks, Internet services and other electronic devices can be accomplished as appropriate supervision is available. After completing a training session, students will be able to use a variety of applications—including electronic mail (email), Usenet News and the World Wide Web etc. The following are required of all students before access will be granted.

1. A yearly signed permission form must be on file at the school.

2. All users must complete the training provided by the school.

3. Usage is limited to school projects and school-related material/activities.

4. Students are expected to follow school rules and act as positive representatives of the school while on the Internet or other wireless devices.

. 5. All users are expected to abide by generally accepted rules of network/wireless etiquette.

6. Transmission of any material in violation of national or state regulation is prohibited.

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 services and other electronic devices.

C. **Prohibited Use**

The user is responsible for his/her actions and activities involving school unit computers, networks, Internet services any other electronic device used on the school premises, 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, bullying, discriminatory, harassing and/or illegal;

2. **Illegal Activities** – Using the school unit's computers, networks, Internet services or other electronic devices (i.e. cell phones, etc.) for any illegal activity that violates other Board policies, procedures and/or school rules;

3. **Violating Copyrights** – Copying or downloading copyrighted materials without the owner's permission;

4. **Plagiarism** – Representing as one's own work any materials obtained on the Internet or other wireless electronic devices (such as term papers, articles, tests, 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;

6. **Non-School-Related Uses** – Using the school unit's computers, networks, Internet services and other electronic devices for non-school-related purposes such as private financial gain, commercial, advertising or solicitation purposes, or for any other personal use;

7. **Misuse of Passwords/Unauthorized Access** – Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts;

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

9. **Unauthorized Access to Chat Rooms/News Groups** – Accessing chat rooms or news groups without specific authorization from the supervising teacher

D. **No Expectation of Privacy**

The school unit retains control, custody and supervision of all computers, networks, Internet services and other electronic devices

owned or leased by the school unit. Furthermore, the school unit reserves the right to monitor all computer, Internet activity and other wireless or personal electronic devices used by students at school. 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 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 services and other electronic devices is a high priority. Any user who identifies a security problem must notify the system 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, networks, Internet services and other electronic devices.

Cross Reference: IJNDB – Student Computer, Internet, and Electronic Devise Use

Original: 03-19-97
1st Reading: 01-02-07
2nd Reading and Adoption to Replace Original: 02-13-07
Amended: 1-11-12
First Reading: 1-31-12
Adopted: 2-28-12

NEPN/NSBA Code: IJNDB-E

**MILLINOCKET SCHOOL DEPARTMENT**
**STUDENT COMPUTER/INTERNET USE ACKNOWLEDGMENT FORM**

No student shall be allowed to use school computers, networks, Internet services and other electronic devices until the student and parent/guardian have signed and returned this acknowledgment to the school.

**Student: _____**
**(Please print student's name)**

I have read policy IJNDB – Student Computer, Internet, and Electronic Device Use and IJNDB-R – Student Computer/Internet Electronic Device Use Rules and agree to comply with them.

_____ _____
Signature of Student Date

**Parent/Guardian: _____**
**(Please print parent/guardian's name)**

I have read policy IJNDB – Student Computer, Internet and Electronic Device Use and IJNDB-R – Student Computer, Internet and Electronic Device Rules and understand that my son/daughter's use of school computers, networks, Internet services and other electronic devices is subject to compliance with these rules.

_____ _____
Signature of Parent/Guardian Date