

Code: IJNDB-R  
Adopted 2/10/03  
Amended 3/20/06  
Amended: 4/9/12

Hermon School Department

## **Student Computer and Internet Use Rules**

These rules accompany Hermon School Committee policy IJNDB (Student Computer and Internet Use). Each student is responsible for his/her actions and activities involving Hermon School Department computers, networks and Internet services, and for his/her computer files, passwords and accounts. These rules provide general guidance concerning the use of the School Department's computers 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 a building administrator or the technology coordinator.

### **A. Consequences for Violation of Computer Use Policy and Rules**

Student use of School Department computers, networks and Internet services is a privilege, not a right. Compliance with the School Department'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, revoked, or restored based upon the circumstances of the particular case, the student's prior disciplinary record and any other pertinent factors.

In cases which the violation affects the integrity of the network, the Information Services (I.S.) Department may also suspend or revoke the student's privileges. The I.S. Department may restore the privileges with the approval of the building principal.

### **B. Acceptable Use**

The School Department's computers, networks and Internet services are provided for educational purposes and research consistent with the School Department's educational mission, curriculum and instructional goals.

All School Committee policies, school rules and expectations concerning student conduct and communication 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 School Department's computers.

### **C. Prohibited Uses**

Examples of unacceptable use of School Department 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 aggressive, threatening, discriminatory, harassing and/or illegal materials.
2. **Illegal Activities** - Using the School Department's computers, networks and Internet services for any illegal activity or in violation of any School Committee policy or school rules. The School Department assumes no responsibility for illegal activities of students while using school computers.
3. **Violating Copyrights** - Copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission (See School Committee policy EGAD - Copyright Compliance). The School Department assumes no responsibility for copyright violations by students.
4. **Copying Software** - Copying, downloading or installing 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. The School Department assumes no responsibility for illegal software copying by students.
5. **Plagiarism** - Representing as one's own work any materials 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 School Department's computers, networks and Internet services for non-school-related purposes such as private financial gain; commercial, advertising or solicitation purposes; and 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 School Department's computers, networks and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses.
9. **Unauthorized Disclosure of Personal Information** – Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.
10. **Unauthorized Access to Blogs/Chat Rooms by Students** - Accessing chat rooms without specific authorization from the supervising faculty member.
11. **Use of Personal Computers Computing Devices** - Any use of personal computing devices without obtaining prior consent through an application process established by the superintendent.

**D. No Expectation of Privacy**

The Hermon School Department computers remain under the control, custody and supervision of the School Department at all times. Students have no expectation of privacy in the use of any computing device in the school district, including e-mail, stored files and Internet access logs. In the event that a staff member has reasonable suspicion that a personal computing device is being used in violation of this policy, the district shall have the right to inspect the device.

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

The student and his/her parents are responsible for compensating the School Department for any losses, costs or damages incurred by the School Department for violations of School Committee policies and school rules while the student is using School Department computers or personal computer equipment on the school network, including the cost of investigating such violations. The School Department assumes no responsibility for any unauthorized charges or costs incurred by a student while using School Department computers or the network.

**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 Department'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 subject to disciplinary and/or legal action in addition to having his/her computer privileges limited, suspended or revoked.

## **H. Additional Rules for Laptops Issued to Students**

1. Laptops, which are loaned, shall be used for educational purposes only and not be used to engage in activities of no educational value.
2. Before a laptop is issued to a student, the student and/his/her parent must sign the school's acknowledgment form. In connection with laptops under the Maine Learning Technology Initiative (MLTI), parents are required to attend an informational meeting before a laptop will be issued to their child.
3. Students and faculty are responsible for the proper care at all times, including costs associated with repairing or replacing the laptop. The school may establish or offer an insurance policy to protect the laptop.
4. If a laptop is lost or stolen, this must be reported to the building principal immediately. If a laptop is stolen, a report should be made to the local police and to the building principal immediately.
5. The School Committee's policies or rules governing the use of any computer, or any careless use of any laptop may result in a student's laptop being confiscated and/or a student only being allowed to use the laptop under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of School Committee policies or school rules.
6. 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.
7. Laptops must be returned in acceptable working order at the end of the school year or whenever requested by staff.

Cross Reference: IJNDB - Student Computer and Internet Use

