

## STUDENT COMPUTER AND INTERNET USE RULES

These rules implement School Committee 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. Failure to comply with School Committee Policy IJNDB and these rules may result in loss of computer and Internet 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 and Internet 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 and Internet services are provided for educational purposes and research 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 and Internet services.

Information Service Department will be consulted before any special computer hardware, other than what is stated above, is purchased. This will insure that such hardware will work properly with the Windham School Department network

### C. Prohibited Use

The user is responsible for his/her actions and activities involving school unit computers, networks and Internet 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, pornographic, harassing and/or illegal;
- 2. Illegal Activities:** Using the school unit's computers, networks and Internet services for any illegal activity or that violates other School Committee policies, procedures and/or school

- rules such as, but not limited to: harassing communications/behavior, discriminatory communications/behavior, any use involving materials that are obscene, pornographic, sexually explicit, or sexually suggestive;
3. **No outside hardware:** Prior permission will be sought from the Information Service Department before any outside equipment is plugged into the district's network, such as personal laptops or handheld devices;
  4. **Computer accessories and equipment:** Any computer accessory or equipment not explicitly defined by this policy is prohibited without prior permission from the Information Service Department. Examples would include USB memory sticks or external hard drives or CD/DVD devices;
  5. **Violating Copyrights:** Copying or downloading copyrighted materials without the owner's permission;
  6. **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 Web site must be identified;
  7. **Copying Software:** Copying or downloading software without the express authorization of the system administrator;
  8. **Non-School-Related Uses:** Using the school unit's computers, networks and Internet services for non-school-related purposes such as private financial gain; commercial, advertising or solicitation purposes, or for any other personal use;
  9. **Misuse of Passwords/Unauthorized Access:** Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts;
  10. **Malicious Use/Vandalism:** Any malicious use, disruption or harm to the school unit's computers, networks and Internet services, including, but not limited to, hacking activities and creation/uploading of computer viruses;
  11. **Unauthorized Access to E-mail, Message Board, Chat Rooms, and/or News Groups:** Attempt to access e-mail, message boards, chat rooms or news groups without specific authorization from the supervising teacher;
  12. **Representation of Personal Views:** Any communication that represents personal views as those of the school unit or that could be misinterpreted as such;
  13. **Accessing Computers While Privileges are Revoked:** Using school computers, networks and Internet services after such access has been denied or revoked;
  14. **System Security:** Failing to report a known breach of computer security to the system administrator.

15. **Deleting/Concealing Inappropriate Information:** Any attempt to delete, erase, or conceal any information stored on a school computer that violates these rules.

**D. No Expectation of Privacy**

The school unit 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 computer and Internet activity by students. Students have no expectation 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 and Internet services 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 Acknowledgment Required**

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

Cross Reference: IJND – Web Site Policy  
IJNDB – Student Computer and Internet Policy  
GCSA – Employee Computer and Internet Policy

Adopted: April 28, 2004