Policy IJNDB-R - Student Computer and Internet Use Rules

These rules accompany Board policy IJNDB (Student Computer and Internet Use). Each student is responsible for his/her actions and activities involving school unit computers (including computing devices issued to students), networks, and Internet services, and for his/her computer files, passwords, accounts and personal computing devices accessing the West Bath School Administrative Unit (WBSAU) network.

These rules provide general guidance concerning the use of the school unit's computing devices 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. Acceptable Use

The school unit's computing devices, networks, and Internet services are provided for educational purposes and research consistent with the school unit's educational mission, curriculum, and instructional goals.

All Board policies, school rules, and expectations concerning student conduct and communications apply when students are using the school unit's computing devices, whether it is on or off school property.

Students are also expected to comply with all specific instructions from school administrators, school staff or volunteers when using the school unit's computing devices.

B. Consequences for Violation of Computer Use Policy and Rules

Student use of the school unit computing devices, networks, and Internet services is a privilege, not a right. Compliance with the school unit's policies and rules concerning computer use is mandatory. Students who violate these policies and rules may, after having been given the opportunity to respond to an alleged violation, 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 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 relevant factors.

C. Prohibited Uses

Examples of unacceptable uses of school unit computing devices that are expressly prohibited include, but are not limited to, the following:

1. **Accessing or Posting 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 or engaging in "cyber bullying";

2. **Illegal Activities** – Using the school unit's computing devices, networks, and Internet services for any illegal activity or in violation of any Board policy or school rules. The school unit assumes no responsibility for illegal activities of students while using school computing devices;

3. **Violating Copyrights** – Copying, downloading or sharing any type of copyrighted materials (including music or films) without the owner's permission (see Board policy/procedure EGAD – Copyright Compliance). The school unit assumes no responsibility for copyright violations by students;

4. **Copying Software** – Illegal unauthorized copying of software may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for illegal software copying by students;

5. **Plagiarism** – Representing as one's own work any materials obtained on the Internet (such as term papers, articles, music, etc.). When Internet sources are used in student work, the author, publisher, and website must be identified;

6. **Non-School-Related Uses** – Using the school unit's computing devices, networks, school accounts, and Internet services for non-school-related purposes such as private financial gain, commercial, advertising or solicitation purposes, or for 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 unit's computing devices, networks, and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses; and

9. **Access to Blogs/Chat Rooms/Social Networking Sites** – Accessing blogs, chat rooms or social networking sites to which student access is prohibited.

D. **No Expectation of Privacy**

The WBSAU computing devices remain under the control, custody, and supervision of the school unit at all times. Students should have no expectation of privacy in their use of school computing devices, including email, stored files, and Internet access logs.

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

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

F. **Student Security**

A student is not allowed to reveal his/her full name, address or telephone number, social security number, or other personal information on the Internet without prior permission from a school official. 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 unit's computing devices, 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.

Cross Reference:

EGAD – Copyright Compliance
IJNDB – Student Computer and Internet Use
IJNDB-R - Student Computer and Internet Use Rules
IJDNB-E(1) - Internet Network Access Agreement - Students
IJDNB-E(2) - Internet Network Access Agreement - Parents/Guardians
IJNDC-E - Agreement to Publish Student Information on School Department Websites
IJNCD-E(2) - Parent/Guardian Agreement Form to Publish Student Information on School Department Websites
GCSA – Employee Computer and Internet Use
JICK - Bullying

First Reading: 08/17/15
Second Reading: 09/02/15
Adopted: 09/02/15
Revised: 8/15/18