

IJNDB-R Student Computer and Internet Use Rules

STUDENT COMPUTER AND INTERNET USE RULES

These rules accompany Board policy IJNDB (Student Computer and Internet Use and Internet Safety). Each student is responsible for their actions and activities involving school unit computers (including I-Pads, tablets, laptops and other devices issued to students), networks and Internet services, and for their computer files, passwords, accounts.

These rules provide general guidance concerning the use of the school unit's computers and networks 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 Director.

Acceptable Use

The school unit's computers, network 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 school resources, whether use 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 computers and networks.

Consequences for Violation of Computer and Internet Use Policy and Rules

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 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.

Prohibited Uses

Examples of unacceptable uses of school unit computers and networks that are expressly prohibited include, but are not limited to, the following:

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 messages. engaging in “cyber bullying”; Illegal Activities – Using the school unit’s computers, 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 computers and networks; 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;

Copying Software – Copying or downloading software without the express authorization of the Technology Director. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for illegal software copying by students; Downloading “Apps” – Students may not download any “apps” without prior approval from an authorized school employee. 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. Non-School-Related Uses – Using the school unit’s computers, networks and Internet services for any personal use reasons not connected with the educational program or assignments. Misuse of Passwords/Unauthorized Access – Sharing passwords, using other users’ passwords, and accessing or other users’ accounts; Malicious Use/Vandalism – Any malicious use, disruption or harm to the school unit’s computers, network and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses: and Unauthorized Access to Blogs/Chat Rooms/Social Networking Sites – Accessing blogs, chat rooms or social networking sites to which student access is prohibited.

No Expectation of Privacy

Regional School Unit 1 computers and networks remain under the control, custody, and supervision of the school unit at all times. Students have no expectation of privacy in their use of school computers and networks, including email, stored files, and Internet access logs. Students should have no expectations of privacy while accessing the school network from school or personal computers and devices.

Compensation for Losses, Costs, and/or Damages

The student and their 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 computers and networks, 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 computers and networks.

Student Security

A student is not allowed to reveal their full name, address or telephone number, social security number, or other personal information on the Internet without prior permission from a staff member. 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.

System Security

The security of the school unit's computers, networks and Internet services is a high priority. Any student who identifies a security problem must notify their 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 their computer privileges limited, suspended, or revoked.

Additional Rules for Devices Issued to Students

Devices are loaned to students as an educational tool and are only authorized for use in completing school assignments

Before a device is issued to a student, the student must sign the school's "acceptable use" agreement.

Students and their parents are responsible for the proper care of devices at all times, whether on or off school property, including costs associated with repairing or replacing the device.

Loss or theft of a device must be reported immediately to the building principal, and if stolen, to the local law enforcement authority as well.

The Board's policy and rules concerning computer and Internet use apply to use of devices at any time or place, on or off school property. Students are responsible for obeying any additional rules concerning care of devices issued by school staff.

Violation of policies or rules governing the use of computers, or any careless use of a device may result in a student's device being confiscated and/or a student only being allowed to use the device under the direct supervision of school staff. The student will also be subject to disciplinary action for any violations of Board policies or school rules.

Parents are responsible for supervising their child's use of the device and Internet access when in use at home.

The device may only be used by the student to whom it is assigned.

Devices must be returned in acceptable working order at the end of the school year or whenever requested by school staff.

Cross Reference: EGAD – Copyright Compliance IJNDB – Student Computer and Internet Use GCSA – Employee Computer and Internet Use

Adopted: March 16, 2009

Revised: October 22, 2012; March 25, 2024

Revision #3

Created 7 April 2022 15:36:50 by Matt Frey-Davis

Updated 26 November 2024 16:16:46 by Kimberly Burgess