

Computer, Network, and Internet Use Student Policy

(As of 8/1/09)

I. Overview

a. Purpose

The intent of this regulation is to provide students with general requirements for utilizing Buffalo Valley Public School District computers, networks, E-mail, and Internet services. The regulation may be supplemented by more specific administrative procedures and rules governing day-to-day management and operation of the computer system.

These rules provide general guidelines and examples of prohibited uses for illustrative purposes but do not attempt to state all required or prohibited activities by users. Students who have questions regarding whether a particular activity or use is acceptable should seek further guidance from their teacher, principal, or the network administrator.

Failure to comply with the Board policy and/or other established regulation governing computer use might result in disciplinary action, up to and including suspension. Illegal uses of computers may also result in referral to law enforcement authorities. The student shall be responsible for any losses, costs or damages incurred by Buffalo Valley Public School District related to his/her violations of Policy and/or these rules.

b. Those Affected

All student users of the Buffalo Valley Public Schools Network and Computer Systems

II. Personal Responsibility

The Buffalo Valley Public School District is pleased to make available to the students, access to the district network, student E-mail, and the Internet, which provides various means of accessing significant educational materials and opportunities.

In order for the District to continue making its computer network, E-mail, and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network, E-mail, and Internet access may jeopardize the ability of all students to enjoy such access. While the schools' teachers and other staff will make reasonable efforts to supervise student use of network, E-mail, and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

By signing the Student Agreement, students are agreeing not only to follow the rules in this policy, but are agreeing to report any misuse of the network to the person designated by the school for such reporting. Misuse means any violations of this policy or any other use that is not included in the policy, but has the effect of harming the student, another student, or damaging property.

A student who submits to the school a properly signed Agreement and follows the policy to which she or he has agreed will have computer network, E-mail, and Internet access during the time which they are students in the Buffalo Valley Public School District.

III. Acceptable and Prohibited Use

a. Acceptable Use

Student access to Buffalo Valley Public School District computers, networks, E-mail, and Internet services is provided for education, communication, and research purposes. General rules and expectations for student behavior and communication apply to the use of Buffalo Valley Public School District computers, networks, E-mail, and Internet services. If there is any doubt about whether a contemplated activity is educational, students should consult with the person(s) designated by the District to help decide if a use is appropriate.

The level of access that students have to school unit computers, networks, E-mail, and Internet services is based upon specific student learning requirements and needs. Students are to utilize District computers, networks, E-mail, and Internet services for school-related purposes and performance of educational success. Incidental personal use of school computers is permitted as long as such use does not interfere with any student's ability to learn or use the computer for learning, with system operations or other system users. "Incidental personal use" is defined as use by an individual student for occasional personal communications. Students are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

Prohibited Use

The student is responsible for his/her actions and activities involving school unit computers, networks, E-mail, and Internet services and for his/her computer files, passwords and accounts. General examples of unacceptable uses, which are expressly prohibited, include but are not limited to the following:

1. Any use that is illegal or in violation of other Board policies, including harassing, discriminatory or threatening communications and behavior, violating of copyright laws, etc.;
2. Any use that passes confidential or personal information about another individual or group;
3. Any use in which one individual portrays him/herself as another individual for any purpose.
4. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive;
5. Any use that prompts or promotes the buy, selling, or participation in illegal use of any controlled or illegal substances;
6. Any use that prompts or promotes participation in gang activity or violence, whether gang related or not, against another individual or group for any reason;
7. Any use that prompts or promotes the buy, selling, or possession of illegal weapons or participation in terrorist activities or organizations;

8. Any use for private financial gain, or commercial, advertising or solicitation purposes;
9. No student shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school faculty, students, and/or their families for non-school purposes. Students who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or their appropriate administrator;
10. Any communication that represents personal views as those of Buffalo Valley Public School District or that could be misinterpreted as such;
11. Downloading or loading non-educational software or applications without permission from the system administrator;
12. Opening or forwarding any e-mail attachments (executable files) from unknown sources and/or that may contain viruses;
13. Sending mass e-mails to school users or outside parties for school or non-school purposes without the permission of the system administrator or building principal;
14. Any malicious use or disruption of computer, networks, E-mail, and Internet services or breach of security features;
15. Any misuse or damage to computer equipment;
16. Misuse of the computer passwords or accounts (student or other user);
17. Any communications that are in violation of generally accepted rules of network etiquette and/or basic human decency;
18. Any attempt to access unauthorized sites;
19. Failing to report a known breach of computer security to the system administrator;
20. Using school computers, networks, and Internet services after such access had been denied or revoked;
21. Any attempt to delete, erase or otherwise conceal any information stored on a computer that violates these rules.

IV. Netiquette

All students must abide by rules of network etiquette, which include the following:

- a. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.
- b. Avoid language and uses that may be offensive to other users. Don't use access to make, distribute, or redistribute jokes, stories, or other material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
- c. Don't assume that a sender of e-mail is giving his or her permission to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when it is known that the individual would have no objection.
- d. Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format that the recipient can open.

V. Internet Safety

- a. Individual Responsibility of Parents and Students

All students and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every student must take responsibility for his or her use of the computer network, E-mail, and Internet and avoid these sites. Parents of minors are the best guides to materials to shun. If a student finds that other students are visiting offensive or harmful sites, he or she should report such use to the person designated by the District.

- b. Personal Safety

Students should be safe. In using the computer network, E-mail, and Internet, students should not reveal personal information such as home address or telephone number. Students should not use their real last name or any other information that might allow a person to locate them without first obtaining the permission of a supervising teacher. Students should not arrange a face-to-face meeting with someone they "meet" on the computer network or Internet without their parent's permission. Students should never agree to meet a person they have only communicated with on the Internet in a secluded place or in a private setting.

- c. "Hacking" and Other Illegal Activities

It is a violation of this Policy to use the District's computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

d. Confidentiality of Student Information

Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Students should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. An administrator may authorize the release of directory information, as defined by Oklahoma law.

e. Active Restriction Measures

The District-provided Internet access utilizes filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) pornographic, or (3) harmful to minors. The school will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material, which is inappropriate for minors.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that

- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

VI. No Expectation of Privacy

Buffalo Valley Public School District retains control, custody and supervision of all computers, networks, E-mail, and Internet services owned or leased by the District. Buffalo Valley Public School District reserves the right to monitor inspect, copy, review and store at any time and without prior notice any and all usage of the computer network, E-mail, and Internet access and any and all information transmitted or received in connection with such usage by students and other system users. All files saved to or stored on the computer systems are considered the property of the District and shall be scrutinized as such. Students have no expectation of privacy regarding their use of school computers, including e-mail messages, web pages and stored files.

VII. Warranties/Indemnification

The Buffalo Valley Public School District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any student or his or her parent(s) or guardian(s) arising out of the student's use of its computer networks or the Internet under this policy.

By signing the agreement, students are taking full responsibility for his or her use, and the student who is 18 or older or, in the case of a student under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the School, the District, and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from the student's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the student.

The student or, if the student is a minor, the student's parent(s) or guardian(s) agree to cooperate with the District in the event of the District's initiating an investigation of a student's use of his or her access to its computer network and the Internet, whether that use is on a school computer or on another computer outside the District's network.