PENDLETON COUNTY BOARD OF EDUCATION I. INSTRUCTION File: I.13. Educational Purposes and Acceptable Use of Electronic Resources, Technologies and the Internet	Adopted: October 2, 2012 Last Review: August, 2014

To meet the goal that every high school graduate will be prepared fully for college, other post-secondary education or gainful employment the Board believes that a technology infrastructure should be present in the County schools. In order to meet this goal, 21st century technologies and software resources shall be provided in grades prekindergarten through 12.

Students of all ages and educators as lifelong learners require the necessary skills and access to technology tools to take responsibility for their own learning, to be actively involved in critical thinking and problem solving, to collaborate, cooperate, and to be productive citizens. West Virginia students must develop proficiency in 21st century content, technology tools, and learning skills to succeed and prosper in life, in school, and on the job.

An effective public education system develops students who are globally aware, engaged with their communities, and capable of managing their lives and careers to succeed in a digital world.

The Pendleton County Board of Education believes that technology must be interwoven with educational improvements and personalized learning to accomplish educational goals, increase student achievement and educator efficacy, and provide increased opportunities for lifelong learning.

This policy applies equally to students and school personnel. To the extent practicable, technology resources shall be used:

- To maximize student access to learning tools and resources at all times including during regular school hours, before and after school or class, in the evenings, on weekends and holidays and for public education, non-instructional days and during vacations; and
- For student use for homework, remedial work, independent learning, career planning and adult basic education.

Educational Purposes

The Pendleton County Board of Education agrees with the general goals articulated in *SBP 2460 Educational Purposes and Acceptable Use of Electronic Resources, Technologies and the Internet* and adopts the following educational purposes as guidelines to be followed in the Pendleton County Schools:

- To promote student learning, educators must be equipped to fully integrate technology to transform instructional practice and to support student acquisition of technology skills necessary to succeed, to continue learning throughout their lifetimes, and to attain self-sufficiency.
- Learning powered by technology should enable students to achieve at higher academic levels, master digital content and technologies, access and manage information, communicate effectively, think critically, solve problems, work productively as individuals and collaboratively as part of a team, acquire new knowledge, access online assessment systems, and demonstrate personal accountability, productivity, and other self-directional skills.
- The use of instructional technology should provide greater student access to advanced and additional curricular offerings, including increasing student access to quality virtual courses and online distance educational tools, than could be provided efficiently through traditional on-site delivery formats.

- Educators should integrate technology resources to personalize learning, enhance instruction, implement multiple technology-based learning strategies, implement high quality digital content and assessments, and utilize digital resources, technologies, and the Internet in the classroom.
- Technology will enable educators to participate in online professional development, access digital resources and platforms, utilize educational data, and deliver instruction through blended learning and other virtual options. The acceptable use of digital resources and devices is necessary to support a personalized learning landscape and other district and state educational policies.
- The promotion of acceptable use in instruction and educational activities is intended to provide a safe digital environment, as well as meet Federal Communications Commission (FCC) guidelines and E-rate audits.

Home

(P) I.13.1. Digital Citizenship

It is incumbent upon the students and staff to work cooperatively to assure that all technology and digital resources will be utilized appropriately, safely and civilly. Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world and use technology responsibly. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career.

All users need to be part of this digital citizenry to appropriately and safely learn, work, play, and live in today's global society. The International Society for Technology in Education (ISTE) has identified nine elements of digital citizenship:

- Digital Access - full electronic participation in society.
- Digital Commerce - the buying and selling of goods online.
- Digital Communication - the electronic exchange of information.
- Digital Literacy - the capability to use digital technology and knowing when and how to use it.
- Digital Etiquette - the standards of conduct expected by other digital technology users.
- Digital Law - the legal rights and restrictions governing technology use.
- Digital Rights and Responsibilities - the privileges and freedoms extended to all digital technology users and the behavioral expectations the come with them.
- Digital Health and Wellness - the elements of physical and psychological well-being related to digital technology use.
- Digital Security - the precautions that all technology users must take to guarantee their personal safety and the security of their networks.

Digital Etiquette

Users are expected to abide by the generally accepted rules of digital/network etiquette. These include, but are not limited to, the following:

- Be polite. Do not write or send abusive messages to others.
- Use proper English and appropriate language; avoid "Netspeak." Do not swear; do not use vulgarities or other inappropriate language.
- Use extreme caution when revealing personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, and e-mail or as content on any other electronic medium.
- Do not reveal, on any electronic medium, personal information about another individual.
- Do not use the Internet in a way that would disrupt the use of the Internet by others (e.g., downloading huge files during prime time; sending mass e-mail messages; annoying other users).
- Keep educational files and e-mail messages stored on servers to a minimum.
- Activate the appropriate automatic reply message and unsubscribe to listservs if account is to be unused for an extended period of time.

- Only publish student pictures or names on class, school or district web sites that are part of the district/school directory information or when appropriate permission has been obtained. (Also see *File: S.17. Student Permanent Records: Collection, Maintenance and Disclosure*
- Notify the appropriate school authority of any dangerous or inappropriate information or messages encountered.

Digital Security

Students and staff members who identify a security problem on the system must notify a system administrator immediately.

- Users must not demonstrate the problem to other users.
- Users must not use another individual's account or give their passwords to others. Unauthorized attempts to log into the system as a system administrator will result in revocation of user privileges based on state, county or school policies.
- Any user identified as a security risk or having a history of problems with other computer systems may be denied access by the appropriate disciplinary authority.
- The WVDE is the proprietor of a class B license of Internet Protocol (IP) addresses. These addresses include 168.216.000.001 through 168.216.255.255. All addresses are assigned, maintained and managed by the WVDE. Any unauthorized use is strictly prohibited

Home

(P) I.13.2. Accountability and Responsibility

The acceptable and appropriate use of telecommunications and/or access to the Internet and digital resources is an extension of the educator's responsibility in his/her classroom. Educators occupy a position of trust and stand in the place of a parent or guardian while a student is in school. (WVC § 18A-5-1(a). Therefore, it is the educator's responsibility to ensure classroom activities focus on appropriate and specific learning goals and objectives for personalized learning when using Internet-related technologies.

Student use of Internet-related or web-based applications must be authorized by the educator and parent or guardian through *(P) I.13.9 Acceptable use Policy Agreement and Parent Permission Form.* It is also the educator's responsibility not to use electronic technologies in a manner that risks placing him/her in a position to abuse that trust. Even though "educators" are the ones who come in daily classroom contact with students, acceptable/appropriate uses of online resources, technologies and the Internet is a responsibility of **all** educational staff and employees.

(P) I.13.2.1. Pendleton County Board of Education Responsibilities

Pursuant to SBP 2460, Pendleton County Schools shall form a county technology team which will be charged with the responsibility of formulating a comprehensive technology plan that shall be included as part of the Five-Year Online Strategic Plan. In addition to the county technology director, the technology team shall be representative of areas including instruction, finance, facilities, personnel and others as designated by the Superintendent.

As a part of the policy development process, prior to the adoption of an Internet Safety Policy, the Pendleton County Board of Education will provide reasonable notice and hold at least one public hearing or meeting to address the specifics of the proposed Internet Safety Policy acceptable use policy. This shall be accomplished by the Superintendent placing the proposed policy on the official agenda of a Board Meeting to allow for public discussion and input.

SBP 2460 Educational Purposes and Acceptable Use of Electronic Resources, Technologies and the Internet also requires the Board to fulfill the following responsibilities:

- Policy 2520.14 shall be included in all programs of study and at all grade levels.
- The Board shall, whenever possible, make available facilities and technology to accommodate distance learning and access to virtual courses provided through the West Virginia Virtual School and approved course providers.
- The Board, in cooperation with schools, shall, to the extent practicable and as funds and other resources are available, provide students (including those enrolled in adult basic education), teachers, parents and citizens access to technology, in the public schools during non-school hours and in accordance with E-rate guidelines.
- The Board shall provide professional development in the use of technology and its application in the teaching and learning process.
- The Board shall implement appropriate policies to help ensure the safety of students and acceptable use of electronic resources, technologies and the Internet and are encouraged to define a student code of conduct or set of responsibilities to include in acceptable use policies.
- The Board shall provide adequate technology personnel to implement appropriate policies and manage county/school networks to help ensure the safety of students and acceptable use of electronic resources, technologies and the Internet.
- In accordance with W. Va. Code, school aid formula and local funding opportunities, The Board shall provide support for schools to employ Technology Integration Specialists (TIS) and Technology Systems Specialist (TSS). The role of the TIS is to:
  - implement and aid educators with technology integration and fluency;
  - manage/repair school local area networks and connected devices;
  - ensure the safety of students and acceptable use of electronic resources, technologies, and the Internet;
  - implement school policies through technology integration/fluency by the TIS;
  - manage/repair school local area networks through TSS; and
  - ensure the safety of students and acceptable use of electronic resources, technologies and the Internet.
- The use and administration of a network server for Internet connection within the county or school is the responsibility of the designated/approved educator(s) and net administrator(s) at the location of the server. It is their responsibility to ensure that all activities and/or functions of the server involve appropriate school activities. All administrative functions and/or file maintenance to the server are the responsibility of the designated/approved educator/net administrator serving that location.
- All remote access to servers located within the county or school building and connected to a wide area network and/or the Internet is the responsibility of the net administrator(s) and/or educator(s) identified as responsible for the servers. Remote access of any kind is to be used only when specific educational goals have been identified and is not to be in direct competition with local Internet service providers. Additionally, all remotely accessed servers must not conflict with federal, state and local guidelines for appropriate Internet access.
- Server administrators or technical contacts requesting domain names for local servers must apply to the WVDE through an application process. Those receiving a domain name must follow all guidelines detailed as part of the application process, including the adoption of a current safety and acceptable use policy.
- The WVDE and approved service provider(s) can monitor only the e-mail accounts issued to the "access.k12.wv.us" server, which is administered by WVDE and approved provider(s). Non-"access.kI2.wv.us" e-mail accounts should not be used for school/educational purposes. <u>All liability for any non-"access.k12.wv.us" email accounts lies with the administrator(s) and/or educator(s) responsible for student utilization of alternative accounts or the administrator(s) and/or educator(s) identified as responsible for the server being used.</u>
- Only publish student pictures or names on class, school or district web sites that are part of the district/school directory information or when appropriate permission has been obtained. (Also see *File: S.17.Student Permanent Records: Collection, Maintenance and Disclosure.)*

- Districts and schools subject to CIPA may not receive the E-rate discounts unless they certify that they have an Internet Safety Policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors.
- Districts and schools subject to CIPA are required to adopt and implement an Internet Safety Policy addressing: (a) access by minors to inappropriate matter on the Internet; (b) the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) measures restricting minors' access to materials harmful to them.
- District Internet Safety Policies must include the monitoring and filtering of the online activities of students. Internet safety policies must provide for educating students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. The WVDE provides a method and curriculum modules that allow districts/schools to certify compliance with this FCC regulation.
  (See http://wvde.state.wv.us/technology/cipa-compliance.htm)
- Pendleton County Schools' equipment that is used off site is subject to the same rules as when used on site.
- Students and staff are expected to use state, district, and school-owned technology in a responsible, efficient, ethical, and legal manner in accordance with the educational mission of the state, district, and school. The use of such technologies may be restricted or revoked for inappropriate behavior or use.
- Students and staff are encouraged to use district and school equipment whenever possible. However, unauthorized or unacceptable use of personal technology devices by students may result in suspension or revocation of personal device privileges. These uses include, but are not limited to, the following:
  - Using personal devices to gain or give an advantage in a testing situation.
  - Using personal devices during class that are not approved by the school or the individual teacher (e.g. cell phones, smart phones, tablets, digital cameras, MP3 players, and laptops).
  - Downloading and installing district licensed software on personal devices unless specifically allowed by the licensing agreement.
  - Using personal devices to bypass filtering, circumvent network security, or in violation of the acceptable use standards which normally apply to district-owned technology.
  - Using personal devices for violations related to cyber bullying and harassment.
- Pendleton County Schools will provide professional development and classroom lessons regarding the compliance with copyright laws.
- Pendleton County Schools shall keep educational files and e-mail messages stored on servers to a minimum. Users should responsibly back up their data and files. The Board reserves the right to set individual storage limits per server.

Home

(P) I.13.2.2. Individual School Responsibilities

In the current technological society in which we live, it becomes even more incumbent upon each and every person within our local schools to become more technologically skilled and to be vigilant to the dangers that can be encountered when complacency sets in. It is the expectation of the Pendleton County Board of Education that in all school locations that students, parents, administrators and staff will work cooperatively to maintain a safe and professional technological environment within the schools.

To that end, local school administrators shall assume a leadership role in assuring that the following responsibilities are met within their schools:

- The Local school improvement councils shall include in the Five-Year Online Strategic Plan mechanisms to foster the use, to the extent practicable and as funds and other resources are available, of school facilities for the purpose of accessing technology, by students, teachers, parents and citizens during non-school hours and in accordance with E-rate guidelines.

- Every school shall have a school technology team and a comprehensive technology plan that is part of the Five-Year Online Strategic Plan. Schools may choose to have the local school improvement councilor the faculty senate or the curriculum team may serve as the technology team.
- Policy 2520.14 shall be taught and utilized throughout all the programs of study and at all grade levels.
- The Five-Year Online Strategic Plan will include necessary professional development to enable teachers to incorporate technology into the classroom.
- With connections to computers and people all over the world also comes the availability of material that may not be considered to be appropriate or have educational value. On a global network, it is impossible to restrict access to all controversial materials. It is the responsibility of the student, parent, teacher and administrator to follow the acceptable use policies, as well as state and federal laws, so that access to telecommunication networks, computers and the Internet provided by the school, county, RESA and state educational systems is not abused.
- Schools must enforce the use of filtering or electronic technical protection measures during any use of the computers/devices to access the Internet. Encryption of all wireless access points for E-rated Internet access provided via the K-12 network or otherwise is required.
- Schools must follow the guidelines of CIPA and the Children's Online Privacy Protection federal statutes (COPPA).
- See also school responsibilities that may be listed in association with county boards of education and district responsibilities *((P) I.13.2.1.)* and educator, service personnel and staff responsibilities (*(P) I.13.2.3.*).

Home

(P) I.13.2.3. Educator, Service Personnel and Staff Responsibilities

Collaboration, resource sharing, and student/teacher, student/student, and teacher/parent dialogue can all be facilitated by the use of social media and other electronic communication. Such interactivity outside of the school walls can greatly enhance face-to-face classes. However, it is imperative that a clear line be drawn between personal social networking and professional/educational networking to protect the safety of the students and the integrity of educational professionals and service staff.

In order to assist educators in maintaining a professional relationship with students and to avoid situations that could lead to inappropriate relationships between school personnel and students, the following regulations apply to all school personnel in public schools and RESAs and to employees of the WVBE and WVDE. Failure to adhere to these regulations may result in disciplinary action and/or loss of licensure:

- School personnel will maintain a professional relationship with all school students, both inside and outside the classroom and while using any form of social media and other electronic communication. Unethical conduct includes but is not limited to:
  - committing any act of harassment as defined by WVBE and/or district policy;
  - committing or soliciting any sexual act from any minor or any student regardless of age;
  - soliciting, encouraging, or consummating a romantic or inappropriate relationship with a student, regardless of the age of the student;
  - using inappropriate language including, but not limited to, swearing and improper sexual comments;
  - taking inappropriate pictures (digital, photographic or video) of students or exchanging any inappropriate pictures with students; or
  - engaging in any other behavior that constitutes a violation of district or county policy or that is detrimental to the health and welfare of students.
- The viewing, storing, transmission or downloading of pornography or sexually suggestive or sexually explicit material or text on a work computer or other electronic storage or communication device, whether at home or at work, by school personnel or anyone else to whom the school personnel has made the computer or other electronic storage or communication device available, is prohibited. This

same prohibition applies to a personal computer or other electronic storage or communication device while at school or a school activity.

- ❖ All information stored within work computers or servers is the property of the state, county or school, and the personnel using such computers/servers/networks have no expectation of privacy with respect to its contents.

With appropriate professional development, educators will promote and model acceptable use, digital citizenship and online responsibility to support personalized learning and digital-age assessments to meet the educational learning policies, including Policy 2520.14, for all students.

Teachers, specialists, and other supervising adults will teach and discuss the appropriate use of electronic resources, technologies and the Internet with their students, monitor their use, and intervene if the uses are not acceptable.

School personnel who receive information via any electronic resource, including a social networking site, that falls under the mandatory reporting requirements of WVC§ 49-6A-2, must report such behavior as indicated in W. Va. Code.

Staff members should be careful not to use copyrighted material in a manner that violates copyright law.

School personnel are responsible for protecting their passwords associated with their computers and e-mail address and must not make them accessible to others.

Home

(P) I.13.3. Use of Electronic Resources, Technology and the Internet

While working within the framework and within the jurisdiction of the State Board of Education and its agents (local school districts), the use of various electronic resources, technology and the internet is a privilege and not a right. Therefore, the following guidelines and restrictions must be read carefully by all users.

- ❖ Unauthorized or unacceptable use of the Internet or any safety violations as part of an educational program by students, educators or staff may result in suspension or revocation of such use.
- ❖ Each student who will access the Internet will be provided acceptable use training and shall have an acceptable use form, signed by a parent or legal guardian, on file at the county/school.
- ❖ School personnel shall also receive acceptable use training.
- ❖ The WVDE provides the network system, e-mail accounts and Internet access as tools for education and administration in support of the WVBE's mission, including student mastery of rigorous subject matter content and acquisition of global skills. Therefore, users should have no expectation of privacy; and the WVDE reserves the right to monitor, inspect, investigate, copy, review and store, without prior notice, information about the content and usage of:
  - ➢ The network and system files;
  - ➢ User files and disk space utilization;
  - ➢ User applications and bandwidth utilization;
  - ➢ User document files, folders and electronic communications;
  - ➢ E-mail;
  - ➢ Internet access; and
  - ➢ Any and all information transmitted or received in connection with networks, e-mail use and web-based tools.
- ❖ No student or staff user should have any expectation of privacy when using the district's network. The WVDE reserves the right to disclose any electronic message, files, media, etc., to law enforcement officials or third parties as appropriate.

- ❖ No temporary accounts will be issued, nor will a student use an Internet account not specifically created for him or her that allows anonymous posting. Based upon the acceptable use and safety guidelines outlined in this document, WVDE, State Superintendent of Schools and provider(s) system administrators will determine what appropriate use is, and their decision is final.
- ❖ The system administrator and/or local teachers may deny users access for inappropriate use. Additionally, violation of use policies could result in loss of access, personal payment of fees incurred, employment discipline, licensure revocation and/or prosecution. Other violations may also be found in *SBP 4373.*
- ❖ The WVDE's administrative information systems, including the West Virginia Education Information System (WVEIS), are to be used exclusively for the business of the respective state, district (county) and school organizations. All information system data are records of the respective organizations. The

  WVDE reserves the right to access and disclose all data sent over its information systems for any purposes. All staff must maintain the confidentiality of student data in accordance with The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).
- ❖ For reasons of privacy, employees may not attempt to gain access to another employee's files in the WVDE's information systems. However, the WVDE reserves the right to enter an employee's information system files whenever there is a business need to do so.
- ❖ Any of these guidelines are to be cognizant of and superseded by FERP A and other appropriate federal and state laws.
- ❖ The WVDE reserves the right to disclose any electronic message, files, media, etc., to law enforcement officials or third parties as appropriate.
- ❖ The WVDE reserves the right to enter an employee's information system files whenever there is a business need to do so.

Home

(P) I.13.4. Internet and Telecommunication Acceptable Use Procedures

The Pendleton County School System embraces the use of technology to promote educational excellence, resource sharing, assist innovative instruction; provide electronic access to a wide range of information and the ability to communicate. The use of the electronic resources, technologies and the Internet must be in support of education and consistent with the educational goals, objectives and priorities of the WVBE. Use of other networks or computing resources must comply with the rules appropriate for that network and for copyright compliance. Users must also be in compliance with the rules and regulations of the network provider(s) serving West Virginia counties and schools

As the use of telecommunication networks by students increase, there is a need to clarify acceptable use and safety of those networks and to include federal regulations from the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA).

The use of telecommunications and/or access to the Internet is an extension of the students' responsibility in the classroom and must follow all federal and state laws as well as state and local policies.

State, district and school-owned technologies are to be used to enhance learning and teaching as well as improve the operation of the district and school.

Safety measures must be enforced to carry out policies at the state, RESA, county, and school to implement the intent of CIPA, COPPA, E-rate guidelines, FERPA, and any other applicable state and federal statute and policy. (See also *SBP 4373* and WVC §18-2C-2.)

The use of the Internet as part of an educational program is a privilege, not a right, and inappropriate or unauthorized use or safety violations could result in revocation or suspension of that privilege. Each student who will access the Internet will be provided acceptable use training and shall have an acceptable use form, signed by a parent or legal guardian, on file.

Acceptable network use by students and staff includes the following:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of student personalized academic learning and educational administration;
- Appropriate participation in school-sponsored blogs, wikis, web 2.0+ tools, social networking sites and online groups;
- With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff use of the network for incidental personal use in accordance with all district/school policies and guidelines.

At no time should a student be given administrative responsibilities for a server with a wide area network or Internet connection.

Home

(P) I.13.5. Unacceptable use of the Internet and Telecommunications

While the Board always prefers to address its policies in positive terms, it is essential that students and staff be made aware that inappropriate use or transmission of any material in violation of any U.S. or state law, State Board Policy, county policy or regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening, abusive, or obscene material, or material protected by trade secrets. Such inappropriate behavior shall be met with zero tolerance.

In addition, use for commercial activities by for-profit institutions is not acceptable. Use for product advertisement or political lobbying is also prohibited. Illegal activities and privacy and safety violations of COPPA, CIPA and FERPA are strictly prohibited.

Specific examples of unacceptable and/or unauthorized use include, but are not limited to:

- Viewing, creating, accessing, uploading, downloading, storing, sending, or distributing obscene, pornographic or sexually explicit material.
- Downloading, uploading and/or executing viruses, worms, Trojan horses, time bombs, bots, malware, spyware, SP AM, etc., and changes to tools used to filter content or monitor hardware and software.
- Using e-mail and other electronic user IDs/passwords other than one's own. Passwords are the first level of security for a user account. E-mail and system logins and accounts are to be used only by the authorized owner of the account, for authorized purposes. Students and staff are responsible for all activity on their account and must not share their account IDs and passwords.
- Illegally accessing or attempting to access another person's data or personal system files or unauthorized access to other state/district/school computers, networks and information systems.
- Supplying your password and user information to any electronic request or sharing them with others via any other communications.
- Storing passwords in a file without encryption.
- Using the "remember password" feature of Internet browsers and e-mail clients.
- Leaving the computer without locking the screen or logging off.
- Corrupting, destroying, deleting, or manipulating system data with malicious intent.
- Requesting that inappropriate material be transferred.
- Violating safety and/or security measures when using e-mail, chat rooms, blogs, wikis, social networking sites, Web 2.0 tools and other forms of electronic communications.
- Hacking, cracking, vandalizing or any other unlawful online activities.
- Disclosing, using, or disseminating personal information regarding students.
- Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks and other unauthorized uses as referenced in WVBE policies or other policies and laws.
- Personal gain, commercial solicitation and compensation of any kind.

- Any activity which results in liability or cost incurred by the district.
- Downloading, installing and/or executing non-educational gaming, audio files, video files or other applications (including shareware or freeware) without permission or approval.
- Support or opposition for ballot measures, candidates and any other political activity.
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture, etc.).
- Plagiarism or reproducing or repurposing audio/video without permission/consent.
- Attaching unauthorized equipment to the district or school networks. Any such equipment may be confiscated and turned over to law enforcement officers for a potential violation of WVC §61-3C-5, Unauthorized Access to Computer Services.
- Attaching unauthorized equipment or making unauthorized changes to the state backbone network. Unauthorized equipment may be confiscated and may turned over to law enforcement officers for a potential violation of W. Va. Code § 61-3C-5, Unauthorized Access to Computer Services. Only WVDE network personnel may authorize changes which affect the state backbone network.
- Vandalizing technology equipment or data. Vandalism is defined as any attempt to harm or destroy data of another user or to intentionally damage equipment or any connections that are part of the Internet. This includes, but is not limited to, uploading, downloading or creating computer viruses. Vandalism will result in revocation of user privileges.
- Uses related to or in support of illegal activities will be reported to authorities.

(P) I.13.6. State, County and School Networks

The statewide network, the county wide area networks (WANs), and school local area networks (LANs) include wired and wireless computers, peripheral equipment, routers, switches, servers, files, storage devices, e-mail, Internet content, digital tools (blogs, web sites, web mail, groups, wikis, etc.) and any other equipment which communicates via network connections. These components are utilized to provide access to electronic resources, technologies and the Internet. In order that all of these components work in harmony, the State Board of Education has issued the following guidelines:

- The WVDE reserves the right to prioritize the use of and access to the statewide network. Districts may also prioritize local traffic within WANs and LANs consistent with WVDE guidelines.
- All use of the network must support instructional and administrative purposes and be consistent with WVBE policies, WVDE guidelines, E-Rate regulations and state and federal laws.
- A WVDE, approved service provider, and other state agencies operate the statewide infrastructure to provide Internet access for all public schools under the jurisdiction of the WVBE. In accordance with state purchasing guidelines, filtering will be installed at the state network level at the two points of presence (POPs) for Internet access. This will provide filtering for all public schools in a cost effective manner and with efficient management. Providing this service at the state level enables districts to meet CIPA and E-Rate guideline requirements for filtering.
- The district and/or schools may also add additional electronic filters at the local network levels. Other objectionable material may be filtered. The determination of what constitutes "other objectionable" material is a local decision.
- Schools must enforce the use of the filtering or electronic technical protection measures during any use of the network and computers/devices to access the Internet.
- To avoid duplication of effort at the district/school levels, the WVDE will provide a method and instructional modules that allow districts/schools to certify compliance with the new FCC regulations regarding Internet safety policies. The policies must provide for educating students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. Instructional information regarding the WVDE method and curriculum content for certifying that students have been educated about appropriate online behavior can be found at http://wvde.state.wv.us/technology/cipa-compliance.php
- This WVDE method will provide documentation that districts have met the annual E-rate compliance requirements of educating students regarding appropriate use.

(P) I.13.7. Copyrighted Computer Software Use

Copyright laws protect the rights of people who create intellectual property by providing the creator with exclusive rights to license, sell or use the works. A creator owns the rights of reproduction, adaptation, distribution, public performance, public display, digital transmission and moral rights.

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted if and when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, United States Code http://copyright.gov/titlel7) and content is cited appropriately.

The doctrine of fair use for education has developed through court decisions over the years. It has been codified in Section 107 of the United States Copyright Law (Title 17, United States Code), and lists four factors to be considered in determining whether or not a particular use is fair:

- The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes.
- The nature of the copyrighted work.
- The amount and substantiality of the portion used in relation to the copyrighted work as a whole.
- The effect of the use upon the potential market for, or value of, the copyrighted work.

To discourage violation of copyright laws, the following compliance requirements are to be followed by all personnel utilizing County purchased copyrighted computer software.

- Employees and students are expected to adhere to the copyright laws.
- Appropriate software licenses will be obtained for use in a network server system or other multi-access use.
- Programs available through the statewide provisions of technology implementation must comply with stipulations of the various purchase agreements.
- Illegal copies of copyrighted programs shall not be made or used on state, RESA, district or school equipment.
- Students are to be taught the ethical and practical problems and consequences of plagiarism and software/media piracy.
- Employees will be provided yearly reminders of their responsibility through a county chosen procedure to adhere to and enforce the copyright laws and will be provided in-service if necessary.
- Educators and students should perform due diligence by reviewing the Terms and Conditions, Terms of Use, End User License Agreements (EULA), Copyright, etc. prior to utilizing content from resources and software licenses to ensure that they are not violating the Terms and Conditions agreed to of said resource. While Fair Use (Section 107 of the United States Copyright Law, Title 17, United States Code) does allow for some utilization of content, Terms and Conditions may specify the use allowed that would not be defined under Fair Use. (e.g., YouTube does not permit the downloading of video content for use. While showing the video in the classroom could be claimed under Fair Use, the downloading would be prohibited under the terms and conditions and is not defined by Fair Use.)

Under federal law, employees violating the copyright laws may be subject to fines, confiscation of material, and other prosecution. Violations may also result in the employee's suspension and/or dismissal for insubordination under WVC §18A-2-8.

Home

(P) I.13.8. Web Publishing

The Pendleton County Board of Education recognizes the educational benefits of publishing information on the Internet by school personnel and students. The Board also recognizes the importance of guidelines that address content, overall responsibility, potential contributors, quality, technical standards, copyright laws, and student protection. In addressing these issues, the Board declares that its web site and approved school web sites shall adhere to the following web publishing guidelines:

- The "official" Pendleton County web site shall be administered by the person designated by the Superintendent.
- School web sites shall be approved by the Superintendent or his/her designee.
- School web sites shall be administered by the principal or his/her designee.
- Appropriate educational permission must be obtained for student web pages published within the West Virginia public K-12 intranet and from a public K-12 site to the Internet. Helping a community organization develop a web site could be a learning experience/project for students. However, housing a community web site on a school/county server will take K-12 bandwidth and is not recommended and may violate E-rate or other regulations.
- Web site content should:
  - Be appropriate, in good taste, and not harmful to any individual or group.
  - Be grammatically correct, accurately spelled, and have a pleasing appearance.
  - Follow FERPA, state, district and school regulations when using student pictures and names. Parental permission should be obtained. Internet guidelines stress the importance of not publishing the last names of students. Nicknames may be used in place of the given name. Personal information, such as home address, home telephone, credit card information, mother's maiden name, and other personal information should not be published
  - Comply with WVBE policies and regulations.
  - Include information such as an e-mail address of the responsible contact person, copyright, and the last date updated should be included.
  - Remain current, be accurate, and navigation through the site should be easy and user friendly.
  - Restrict business/commercial links or the acknowledgment of a business on a school/county web site to business partners and/or materials that are educational, provide technical support, or are germane to the philosophy of the school/county. Advertising of commercial offerings is forbidden.
  - Comply with copyright, intellectual property, state, federal (specifically COPPA and CIPA) and international law.
  - Include the permission granted statement (who, time period, etc.) for all copyrighted materials.
- Consult the World Wide Web Consortium (W3C) for additional web publishing standards at http://www.w3.orglstandards/webdesign.
- The W3C Web Accessibility Initiative (W AI) develops Web accessibility guidelines. More information is available at http://www.w3.org/WAIlintro/components.php.

Legal resources for all of the forgoing pages are SBP 2460; FCC 11-125, CC docket No. 02-6, GN Docket No. 09-51 and codes cited within the body of the policy.

Home

(P) I.13.9

PENDLETON COUNTY SCHOOLS
ACCEPTABLE USE POLICY AGREEMENT
And
PARENT PERMISSION FORM

School/Location_____

After reading the attached Pendleton County Schools policies, please complete this form to indicate that you agree with the terms and conditions. The signatures of both student and parent/guardian are mandatory before Internet access may be granted. Use of the telecommunications network or telecommunication must be in support of education and/or research or for school business, support of the West Virginia Content Standards and Objectives and be in accordance with all Pendleton County Board of Education policies and SBP 2460.

STUDENT SECTION

I have read the attached policies concerning all computer usage. I agree to follow the rules contained in these policies. I understand that if I violate the rules my privileges may be terminated or other disciplinary action taken.

User Name (please print)_____ Grade: _____

User's Signature: _____ Date: _____

PARENT SECTION

I have read the attached policies concerning the use of telecommunications in my child's school and have discussed this with my son/daughter. I understand that this access is for educational purposes only, and that it is the responsibility of my child to restrict his/her use to the classroom projects/activities assigned by the teacher. I also understand that my child cannot hold the teacher responsible for intentional infractions of the above rules.

Parent/Guardian (please print)-_____

Parent/Guardian (signature) _____Date_____

PERMISSION FORM FOR WORLD WIDE WEB PUBLISHING OR STUDENT WORK

I understand that my child's work or writing may be published on the district's web page at http: /www.pendletoncountyschools.com/. I further understand that no last name, home address or home telephone number will appear with such work. I grant permission for World Wide Publishing. I may withdraw permission in writing at any time.

Student Signature_____ Date: _____

Parent/Guardian Signature: _____ Date:_____

PERMISSION FORM FOR WORLD WIDE WEB PUBLISHING OF STUDENT PHOTOGRAPH

I understand that my child's work or writing may be published on the district's web page at http: /www.pendletoncountyschools.com/. I further understand that no last name, home address or home telephone number will appear with such work. I grant permission for World Wide Publishing. I may withdraw permission in writing at any time.

Student Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date:_____

This form will be kept in the school listed above and signed every year. It will not be transferred to another school.

Legal resources for all of the forgoing pages are SBP 2460; FCC 11-125, CC docket No. 02-6, GN Docket No. 09-51 and codes cited within the body of the policy.

Home

(P) I.13.10.

PENDLETON COUNTY SCHOOLS
ADULT ACCEPTABLE USE POLICY AGREEMENT

School/Location_____

After reading the attached Pendleton County Schools policies, please complete this form to indicate that you agree with the terms and conditions. Use of the telecommunications network or telecommunication must be in support of education and/or research or for school business, support of the West Virginia Content Standards and Objectives and be in accordance with all Pendleton County Board of Education policies and SBP 2460.

ADULT SECTION

I have read the attached concerning all computer usage. I agree to follow the rules contained in these policies. I understand that if I violate the rules my privileges may be terminated or other disciplinary action taken.

User Name (please print)_____

User's Signature: _____ Date: _____

PERMISSION FORM FOR WORLD WIDE WEB PUBLISHING OF EMPLOYEE PHOTOGRAPH /WRITING/WORK

I understand that my work, photograph, or writing may be published on the district's web page at http: /www.pendletoncountyschools.com/. I further understand that no last name, home address or home telephone number will appear with such work. I grant permission for World Wide Publishing. I may withdraw permission in writing at any time.

Employee Signature: _____ Date: _____

Home

PENDLETON COUNTY SCHOOLS
NETWORK AND INTERNET ACCEPTABLE USE POLICY (AUP)

To meet the goal that every high school graduate will be prepared fully for college, other post-secondary education or gainful employment the Board believes that a technology infrastructure should be present in the County schools. In order to meet this goal, 21st century technologies and software resources shall be provided in grades prekindergarten through 12.

Students of all ages and educators as lifelong learners require the necessary skills and access to technology tools to take responsibility for their own learning, to be actively involved in critical thinking and problem solving, to collaborate, cooperate, and to be productive citizens. West Virginia students must develop proficiency in 21st century content, technology tools, and learning skills to succeed and prosper in life, in school, and on the job.

An effective public education system develops students who are globally aware, engaged with their communities, and capable of managing their lives and careers to succeed in a digital world. The Pendleton County Board of Education believes that technology must be interwoven with educational improvements and personalized learning to accomplish educational goals, increase student achievement and educator efficacy, and provide increased opportunities for lifelong learning.

This policy applies equally to students and school personnel. To the extent practicable, technology resources shall be used:

- To maximize student access to learning tools and resources at all times including during regular school hours, before and after school or class, in the evenings, on weekends and holidays and for public education, non-instructional days and during vacations; and
- For student use for homework, remedial work, independent learning, career planning and adult basic education.

Educational Purposes

The Pendleton County Board of Education agrees with the general goals articulated in *SBP 2460 Educational Purposes and Acceptable Use of Electronic Resources, Technologies and the Internet* and adopts the following educational purposes as guidelines to be followed in the Pendleton County Schools:

- To promote student learning, educators must be equipped to fully integrate technology to transform instructional practice and to support student acquisition of technology skills necessary to succeed, to continue learning throughout their lifetimes, and to attain self-sufficiency.
- Learning powered by technology should enable students to achieve at higher academic levels, master digital content and technologies, access and manage information, communicate effectively, think critically, solve problems, work productively as individuals and collaboratively as part of a team, acquire new knowledge, access online assessment systems, and demonstrate personal accountability, productivity, and other self-directional skills.
- The use of instructional technology should provide greater student access to advanced and additional curricular offerings, including increasing student access to quality virtual courses and online distance educational tools, than could be provided efficiently through traditional on-site delivery formats.
- Educators should integrate technology resources to personalize learning, enhance instruction, implement multiple technology-based learning strategies, implement high quality digital content and assessments, and utilize digital resources, technologies, and the Internet in the classroom.
- Technology will enable educators to participate in online professional development, access digital resources and platforms, utilize educational data, and deliver instruction through blended learning and other virtual options. The acceptable use of digital resources and devices is necessary to support a personalized learning landscape and other district and state educational policies.
- The promotion of acceptable use in instruction and educational activities is intended to provide a safe digital environment, as well as meet Federal Communications Commission (FCC) guidelines and E-rate audits.

(P) I.13.1. Digital Citizenship

It is incumbent upon the students and staff to work cooperatively to assure that all technology and digital resources will be utilized appropriately, safely and civilly. Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world and use technology responsibly. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career.

Digital Etiquette

Users are expected to abide by the generally accepted rules of digital/network etiquette. These include, but are not limited to, the following:

- Be polite. Do not write or send abusive messages to others.
- Use proper English and appropriate language; avoid "Netspeak." Do not swear; do not use vulgarities or other inappropriate language.
- Use extreme caution when revealing personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, and e-mail or as content on any other electronic medium.
- Do not reveal, on any electronic medium, personal information about another individual.
- Do not use the Internet in a way that would disrupt the use of the Internet by others (e.g., downloading huge files during prime time; sending mass e-mail messages; annoying other users).
- Keep educational files and e-mail messages stored on servers to a minimum.
- Activate the appropriate automatic reply message and unsubscribe to listservs if account is to be unused for an extended period of time.
- Only publish student pictures or names on class, school or district web sites that are part of the district/school directory information or when appropriate permission has been obtained. (Also see *File: S.17. Student Permanent Records: Collection, Maintenance and Disclosure*
- Notify the appropriate school authority of any dangerous or inappropriate information or messages encountered.

Digital Security

Students and staff members who identify a security problem on the system must notify a system administrator immediately.

- Users must not demonstrate the problem to other users.
- Users must not use another individual's account or give their passwords to others. Unauthorized attempts to log into the system as a system administrator will result in revocation of user privileges based on state, county or school policies.
- Any user identified as a security risk or having a history of problems with other computer systems may be denied access by the appropriate disciplinary authority.
- The WVDE is the proprietor of a class B license of Internet Protocol (IP) addresses. These addresses include 168.216.000.001 through 168.216.255.255. All addresses are assigned, maintained and managed by the WVDE. Any unauthorized use is strictly prohibited

(P) I.13.2. Accountability and Responsibility

The acceptable and appropriate use of telecommunications and/or access to the Internet and digital resources is an extension of the educator's responsibility in his/her classroom. Educators occupy a position of trust and stand in the place of a parent or guardian while a student is in school (WVC § 18A-5-1(a). Therefore, it is the educator's responsibility to ensure classroom activities focus on appropriate and specific learning goals and objectives for personalized learning when using Internet-related technologies.

Student use of Internet-related or web-based applications must be authorized by the educator and parent or guardian through *(P) I.13.4.1 Internet and Telecommunications Access Consent and Waiver Form.* It is also the educator's responsibility not to use electronic technologies in a manner that risks placing him/her in a position to abuse that trust. Even though "educators" are the ones who come in daily classroom contact with students, acceptable/appropriate uses of online resources, technologies and the Internet is a responsibility of **all** educational staff and employees.

(P) I.13.3. Use of Electronic Resources, Technology and the Internet

While working within the framework and within the jurisdiction of the State Board of Education and its agents (local school districts), the use of various electronic resources, technology and the internet is a privilege and not a right. Therefore, the following guidelines and restrictions must be read carefully by all users.

- Unauthorized or unacceptable use of the Internet or any safety violations as part of an educational program by students, educators or staff may result in suspension or revocation of such use.
- Each student who will access the Internet will be provided acceptable use training and shall have an acceptable use form, signed by a parent or legal guardian, on file at the county/school.
- School personnel shall also receive acceptable use training.
- The WVDE provides the network system, e-mail accounts and Internet access as tools for education and administration in support of the WVBE's mission, including student mastery of rigorous subject matter content and acquisition of global skills. Therefore, users should have no expectation of privacy; and the WVDE reserves the right to monitor, inspect, investigate, copy, review and store, without prior notice, information about the content and usage of:
  - The network and system files;
  - User files and disk space utilization;
  - User applications and bandwidth utilization;
  - User document files, folders and electronic communications;
  - E-mail;
  - Internet access; and
  - Any and all information transmitted or received in connection with networks, e-mail use and web-based tools.
- No student or staff user should have any expectation of privacy when using the district's network. The WVDE reserves the right to disclose any electronic message, files, media, etc., to law enforcement officials or third parties as appropriate.
- No temporary accounts will be issued, nor will a student use an Internet account not specifically created for him or her that allows anonymous posting. Based upon the acceptable use and safety guidelines outlined in this document, WVDE, State Superintendent of Schools and provider(s) system administrators will determine what appropriate use is, and their decision is final.
- The system administrator and/or local teachers may deny users access for inappropriate use. Additionally, violation of use policies could result in loss of access, personal payment of fees incurred, employment discipline, licensure revocation and/or prosecution. Other violations may also be found in *SBP 4373.*
- The WVDE's administrative information systems, including the West Virginia Education Information System (WVEIS), are to be used exclusively for the business of the respective state, district (county) and school organizations. All information system data are records of the respective organizations. The
  WVDE reserves the right to access and disclose all data sent over its information systems for any purposes. All staff must maintain the confidentiality of student data in accordance with The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).
- For reasons of privacy, employees may not attempt to gain access to another employee's files in the WVDE's information systems. However, the WVDE reserves the right to enter an employee's information system files whenever there is a business need to do so.
- Any of these guidelines are to be cognizant of and superseded by FERP A and other appropriate federal and state laws.
- The WVDE reserves the right to disclose any electronic message, files, media, etc., to law enforcement officials or third parties as appropriate.
- The WVDE reserves the right to enter an employee's information system files whenever there is a business need to do so.

(P) I.13.4. Internet and Telecommunication Acceptable Use Procedures

The Pendleton County School System embraces the use of technology to promote educational excellence, resource sharing, assist innovative instruction; provide electronic access to a wide range of information and the ability to communicate. The use of the electronic resources, technologies and the Internet must be in support of education and consistent with the educational goals, objectives and priorities of the WVBE. Use of other networks or computing resources must comply with the rules appropriate for that network and for copyright compliance. Users must also be in compliance with the rules and regulations of the network provider(s) serving West Virginia counties and schools

As the use of telecommunication networks by students increase, there is a need to clarify acceptable use and safety of those networks and to include federal regulations from the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA). The use of telecommunications and/or access to the Internet is an extension of the students' responsibility in the classroom and must follow all federal and state laws as well as state and local policies.

State, district and school-owned technologies are to be used to enhance learning and teaching as well as improve the operation of the district and school. Safety measures must be enforced to carry out policies at the state, RESA, county, and school to implement the intent of CIPA, COPPA, E-rate guidelines, FERPA, and any other applicable state and federal statute and policy. (See also *SBP 4373* and WVC §18-2C-2.)

The use of the Internet as part of an educational program is a privilege, not a right, and inappropriate or unauthorized use or safety violations could result in revocation or suspension of that privilege. Each student who will access the Internet will be provided acceptable use training and shall have an acceptable use form, signed by a parent or legal guardian, on file.
Acceptable network use by students and staff includes the following:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of student personalized academic learning and educational administration;
- Appropriate participation in school-sponsored blogs, wikis, web 2.0+ tools, social networking sites and online groups;
- With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff use of the network for incidental personal use in accordance with all district/school policies and guidelines.

At no time should a student be given administrative responsibilities for a server with a wide area network or Internet connection.

(P) I.13.5. Unacceptable use of the Internet and Telecommunications

While the Board always prefers to address its policies in positive terms, it is essential that students and staff be made aware that inappropriate use or transmission of any material in violation of any U.S. or state law, State Board Policy, county policy or regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening, abusive, or obscene material, or material protected by trade secrets. Such inappropriate behavior shall be met with zero tolerance.

In addition, use for commercial activities by for-profit institutions is not acceptable. Use for product advertisement or political lobbying is also prohibited. Illegal activities and privacy and safety violations of COPPA, CIPA and FERPA are strictly prohibited. Specific examples of unacceptable and/or unauthorized use include, but are not limited to:

- Viewing, creating, accessing, uploading, downloading, storing, sending, or distributing obscene, pornographic or sexually explicit material.
- Downloading, uploading and/or executing viruses, worms, Trojan horses, time bombs, bots, malware, spyware, SP AM, etc., and changes to tools used to filter content or monitor hardware and software.
- Using e-mail and other electronic user IDs/passwords other than one's own. Passwords are the first level of security for a user account. E-mail and system logins and accounts are to be used only by the authorized owner of the account, for authorized purposes. Students and staff are responsible for all activity on their account and must not share their account IDs and passwords.
- Illegally accessing or attempting to access another person's data or personal system files or unauthorized access to other state/district/school computers, networks and information systems.
- Supplying your password and user information to any electronic request or sharing them with others via any other communications.
- Storing passwords in a file without encryption.
- Using the "remember password" feature of Internet browsers and e-mail clients.
- Leaving the computer without locking the screen or logging off.
- Corrupting, destroying, deleting, or manipulating system data with malicious intent.
- Requesting that inappropriate material be transferred.
- Violating safety and/or security measures when using e-mail, chat rooms, blogs, wikis, social networking sites, Web 2.0 tools and other forms of electronic communications.
- Hacking, cracking, vandalizing or any other unlawful online activities.
- Disclosing, using, or disseminating personal information regarding students.
- Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks and other unauthorized uses as referenced in WVBE policies or other policies and laws.
- Personal gain, commercial solicitation and compensation of any kind.
- Any activity which results in liability or cost incurred by the district.
- Downloading, installing and/or executing non-educational gaming, audio files, video files or other applications (including shareware or freeware) without permission or approval.
- Support or opposition for ballot measures, candidates and any other political activity.
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture, etc.).
- Plagiarism or reproducing or repurposing audio/video without permission/consent.
- Attaching unauthorized equipment to the district or school networks. Any such equipment may be confiscated and turned over to law enforcement officers for a potential violation of WVC §61-3C-5, Unauthorized Access to Computer Services.

- Attaching unauthorized equipment or making unauthorized changes to the state backbone network. Unauthorized equipment may be confiscated and may turned over to law enforcement officers for a potential violation of W. Va. Code § 61-3C-5, Unauthorized Access to Computer Services. Only WVDE network personnel may authorize changes which affect the state backbone network.
- Vandalizing technology equipment or data. Vandalism is defined as any attempt to harm or destroy data of another user or to intentionally damage equipment or any connections that are part of the Internet. This includes, but is not limited to, uploading, downloading or creating computer viruses. Vandalism will result in revocation of user privileges.
- Uses related to or in support of illegal activities will be reported to authorities.

Home

(P) I.13.11. Sexting by Minors

Any minor who intentionally possesses, creates, produces, distributes, presents, transmits, posts, exchanges, or otherwise disseminates a visual portrayal of another minor posing in an inappropriate sexual manner or who distributes, presents, transmits, posts, exchanges or otherwise disseminates a visual portrayal of himself or herself posing in an inappropriate sexual manner shall be guilty of an act of delinquency and upon adjudication disposition may be made by the circuit court pursuant to the provisions of article five, chapter forty -nine of this code

As used in this policy:

- "Posing in an inappropriate sexual manner" means exhibition of a bare female breast, female or male genitalia, pubic or rectal areas of a minor for purposes of sexual titillation.
- "Visual portrayal" means:
  - A photograph;
  - A motion picture;
  - A digital image
  - A digital video recording; or
  - Any other mechanical or electronic recording process or device that can preserve, for later viewing, a visual image of a person that includes, but is not limited to, computers, cellphones, personal digital assistance and other digital storage or transmitting devices;(c) It shall be an affirmative defense to an alleged violation of this section that a minor charged with possession of the prohibited visual depiction did neither solicit its receipt nor distribute, transmit or present it to another person by any means.

As written, the code allows for court discretion as to whether an adjudicated juvenile should be required to register as a sex offender.

It should be clearly understood that while some of these activities may be initiated outside of the school environment, they will be subject to school discipline under *File: S.8. Expected Behavior in Safe and Supportive Schools* if they disrupt normal school activities.

Students who initiate prohibited activities within the school day, including transportation time, shall be disciplined according to *File: I.13. Educational Purposes and Acceptable Use of Electronic Resources, Technologies and the Internet.*
(WVC §61-8c-3b)

Home

(P) I.13.12. Sexting Educational Diversion Program

Before a juvenile petition is filed for activity proscribed by WVC §61-8a or 8c, or after probable cause has been found to believe a juvenile has committee a violation thereof, but before an adjudicatory hearing on the petition, the court or a prosecuting attorney may direct or allow a minor who engaged in such activity to participate in an educational diversion program. The prosecutor or court may refer the minor to the educational diversion program, as part of a pre-petition diversion and informal resolution; as part of counseling provided; or as part of the requirements of an improvement period to be satisfied in advance of an adjudicatory hearing pursuant to the provisions of section nine of this article.

The educational diversion program to be developed for minors who are accused of activity proscribed by the provisions of WVC §61-8a or 8c will address the following issues and topics:

- The legal consequences of and penalties for sharing sexually suggestive or explicit materials, including
- applicable federal and state statutes;

- The nonlegal consequences of sharing sexually suggestive or explicit materials including, but not limited to, the effect on relationships, loss of educational and employment opportunities, and being barred or removed from school programs and extracurricular activities;
- How the unique characteristics of cyberspace and the Internet, including searchability, replicability and an infinite audience, can produce long-term and unforeseen consequences for sharing sexually suggestive or explicit materials; and
- The connection between bullying and cyber-bullying and minors sharing sexually suggestive or explicit materials.

A minor's successful completion of the program must be considered by the prosecutor and the court in deciding whether to abstain from filing a juvenile petition or dismiss a petition.

- If the minor has not previously been judicially determined to be delinquent, and the minor's activities represent a first offense for a violation of WVC §61-8c-3b, the minor shall not be subject to the requirements of the code, as long as s/he successfully completes the educational diversion program; and
- If the minor commits a second or subsequent violation of article WVC §61-8a or 8c, the minor's successful completion of the educational diversion program may be considered as a factor to be considered by the prosecutor and court in deciding to not file a petition or to dismiss a petition, upon successful completion of an improvement plan established by the court.
  (WVC §49-5-13g)

Home

Amended/Revised: October 1, 2013

PENDLETON COUNTY BOARD OF EDUCATION	Adopted: October 2, 2012
I. INSTRUCTION	Last Review:
File: I.13. 1. Internet Safety Policy	August, 2014

The Children's Internet Protection Act was enacted by Congress to address concerns about access to offensive visual content over the Internet on school and library computers. The Pendleton County Board of Education has those same concerns which are the driving force behind the adoption of this policy.

This policy takes note of the Board's responsibility to protect against Internet access by both adults and minors to visual depictions that are (1) obscene; (2) child pornography; or, with respect to use of the computers by minors, (3) harmful to minors. In addition, section 54.520(c)(1)(i) requires a school to certify that its Internet safety policy includes "monitoring the online activities of minors.

As a part of the policy development process, prior to the adoption of an Internet Safety Policy, the Pendleton County Board of Education will provide reasonable notice and hold at least one public hearing or meeting to address the specifics of the proposed Internet Safety Policy acceptable use policy. This shall be accomplished by the Superintendent placing the proposed policy on the official agenda of a Board Meeting to allow for public discussion and input.

Federal Communications Commission rules require the Board to submit its Internet Safety Policy on or before July 1, 2012 by filing FCC Forms 486 or 479.

Internet Safety Policy Training

All Pendleton County Schools personnel and students involved in any way with the use of technology within the school system shall undergo training on the safe and appropriate use of every type of technology resource. The training may be conducted by knowledgeable staff members within the school system, outside trainers, State Board of Education resources both on line and through department consultants, federal government resources, seminars, workshops off campus and RESA resources.

Existing informational vehicles including, but not limited to, staff development programs, Faculty Senates and Local School Improvement Councils may be utilized for faculty and staff training.

Training programs for students shall be age appropriate and they shall be conducted utilizing the same resources mentioned above for faculty and staff. The training may be integrated with curricular activities, it may be scheduled task specific groups and it may be possible to have after school and weekend workshops.

To avoid duplication of effort at the district/school levels, the WVDE has provided instructional modules that allow districts/schools to certify compliance with the new FCC regulations regarding Internet safety policies. Instructional information is currently provided via TechSteps. Each grade level provides curricular content for teachers to instruct students in compliance with the FCC Guidelines set forth in the Sixth Report and Order. (See http://wvde.state.wv.us/technology/cipa-compliance.php. for additional information and details)

Training shall be ongoing with refresher sessions scheduled as appropriate as determined by the designated Technology Directors.

All clients will receive training on appropriate online behavior, including limited to the following topics:

- Protection measures that block or filter Internet access to images that are: (a) obscene; (b) child pornography or (c) harmful to minors;
- Access by minors to inappropriate materials on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications (social networking);
- Unauthorized access, including so-called "hacking" and other unlawful activities by minors online;
- Unauthorized disclosure, use and dissemination of personal information regarding minors;
- Measures designed to restrict minors' access to materials harmful to them;
- Cyber-bullying awareness and responses;
- Managing and monitoring online activities of minors;
- Proper use and protection of passwords;
- Consequences of Illegally accessing or attempting to access another person's data or personal system files or unauthorized access to other state/district/school computers, networks and information systems;
- Proper care of technology equipment and data (vandalism);
- Digital citizenship; and
- Digital security.

Monitoring the Online Activities of Students

Appropriate adult supervision of Internet use must be provided. The first line of defense in controlling access by students to inappropriate material on the Internet is deliberate and consistent monitoring of student access and use of equipment. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively in filtering and acceptable use issues.

The acceptable and appropriate use of telecommunications and/or access to the Internet and digital resources is an extension of the educator's responsibility in his/her classroom. Educators occupy a position of trust and stand in the place of a parent or guardian while a student is in school. (WVC § 18A-5-1(a).) Therefore, it is the teacher's responsibility to ensure classroom activities focus on appropriate and specific learning goals and objectives for personalized learning when using Internet-related technologies.

While it is true that "teachers" are the ones who come in daily classroom contact with students, the monitoring of acceptable and appropriate uses of online resources, technologies and the Internet is a responsibility of **all** educational staff and employees.

Teachers, specialists, and other supervising adults will not only teach and discuss the appropriate use of electronic resources, technologies and the Internet with their students; they **must** also monitor their use, and intervene if the uses are not acceptable.

No student or staff user should have any expectation of privacy when using the district's network. The WVDE reserves the right to disclose any electronic message, files, media, etc., to law enforcement officials or third parties as appropriate.

School personnel who fail to properly supervise students shall be subject to disciplinary action, licensure revocation and/or prosecution and dismissal if the circumstances warrant such action.

Filtering Electronic Communications

The Pendleton County Board of Education and its agents shall take the steps necessary to assure that all locations within the county enforce the use of filtering or electronic technical protection measures during any use of the computers/devices to access the Internet. Encryption of all wireless access points for E-rated Internet access provided via the K-12 network or otherwise is required.

Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites.

A WVDE, approved service provider, and other state agencies operate the statewide infrastructure to provide Internet access for all public schools under the jurisdiction of the WVBE. In accordance with state purchasing guidelines, filtering will be installed at the state network level at the two points of presence (POPs) for Internet access. This will provide filtering for all public schools in a cost effective manner and with efficient management.

Pendleton County Schools may also add additional electronic filters at the local network levels as it deems appropriate to filter and block other objectionable material which has been identified by the Superintendent or his/her designee.

Any attempts to defeat or bypass the state's Internet filter or conceal Internet activity are prohibited. This includes, but is not limited to, proxies, https, special ports, modifications to state browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content.

E-mail which is inconsistent with the educational missions of the state, district or school will be considered SPAM and blocked from entering e-mail boxes.

Appropriate filtering must be maintained to meet E-rate guidelines.

(SBP 2460; FCC 11-125, CC docket No. 02-6, GN Docket No. 09-51)

Home

Amended/Revised: