PRESTON COUNTY BOARD OF EDUCATION	Adopted: June 11, 2012
FILE: 3 – CURRICULUM AND INSTRUCTION	Last Reviewed:
File: 3-32 Educational Purposes and Acceptable Use of Electronic Resources, Technologies and the Internet	April 2018

Policy 2460 sets forth regulations that apply to districts, schools, students, educators, other school personnel, parents, guardians, WVDE and other users having direct contact with students.
The Preston County Board of Education agrees with the general goals and regulations articulated in SBP 2460 Educational Purposes and Acceptable Use of Electronic Resources, Technologies and the Internet and adopts them as its official policy. This policy shall apply equally to students and school personnel

This policy will assist the school system as it strives to meet local, state and federal statutes and regulations pertaining to safe and acceptable use of the Internet, various digital resources and technologies, compliance with E-rate guidelines, and reinforcement of copyright compliance.

Educational Purposes

The educational purposes set forth within the framework of this policy include but are not limited to:

- 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.
- 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 become proficient in college- and career-readiness standards to succeed and prosper in life, in school, and on the job.
- 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.
- To promote student learning, teachers 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.
- The state, districts, and schools will use electronic resources as a powerful and compelling means for students to learn core and elective subjects and applied skills in relevant and rigorous ways to advance learning as referenced in W. Va. Code §18-2e-7, W. Va. 126CSR44N, WVBE Policy 2520.14, West Virginia College- and Career-Readiness Standards for Technology and Computer Science (Policy 2520.14), W. Va. 126CSR42, WVBE Policy 2510, Assuring the Quality of Education: Regulations for Education Programs, and W. Va. 126CSR44A et al seq., WVBE Policy 2520 series.
- 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 quality virtual courses and online educational tools and resources.
- Teachers should integrate high quality digital content and assessment resources with curriculum to personalize learning.
- 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 both provide a safe digital environment, and meet Federal Communications Commission (FCC) guidelines and E-rate audits.

Home

R 3-32-1 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) includes standards and provides guidance related to digital citizenship for students, teachers, administrators instructional coaches and computer science educators

Digital/Network Code of Conduct:

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, social media, other digital communication platforms, 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).
- Electronic educational material containing confidential student information shall be stored only in secure locations consistent with federal, state, and local privacy regulations. Electronic educational material containing no confidential student information, including but not limited to, lesson plans, worksheets, primary source documents, and other materials used for instruction, may be stored in appropriate locations but should follow state/district guidelines.
- Educators electing to use third party classroom based applications should carefully review the terms of service and privacy policies prior to use for those applications to ensure consistency with best practice. For use of applications with students younger than 13 years of age, recommended best practice is to obtain parental consent prior to use and/or entering any student data. All use of third party applications must be consistent with local policy/guidelines, Family Educational Rights and Privacy Act (20 U.S.C. §1232g; 34 CFR Part 99) FERPA), W. Va. Code §18-2-5h, and W. Va. 126SR94, WVBE
- Activate the appropriate automatic reply message and unsubscribe to listservs if account is to be unused for an extended period of time.
- Appropriate permission shall be obtained prior to publishing student pictures or names on class, school, or district web sites or other publications, provided that such information is not designated as directory information under district policy. All releases of information designated as directory information under district policy must comply with parental opt-out provisions as described in the FERPA and WVBE Policy 4350. (Also see *File: 11-19 Collection, Maintenance and Disclosure of Student Data)*
- Notify the appropriate school authority of any dangerous or inappropriate information or messages encountered.

Digital Security:

Users who identify a security problem on the system must notify a system administrator. Users who are aware of or suspect that confidential information may have been exposed to unauthorized parties must notify district and/or state officials responsible for implementing privacy incident response protocol consistent with federal and state regulations including, but not limited to, Policy 4350 and the Student Data Accessibility, Transparency, and Accountability Act, W. Va. Code §18-2-5h.

- Users must not demonstrate security problems to users other than school district and/or state officials responsible for implementing the privacy incident response protocol.
- 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 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

R 3-32-2 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 *R 3-32-4-1 Internet and Telecommunications Access Consent and Waiver Form.* It is also the educator's responsibility to refrain from using 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.

Adult use of Internet-related or web-based applications must be authorized through the *R 3-32-4-2 Internet and Telecommunications Access Consent and Waiver Form*. Access Passwords cannot be issued to adult users until this form is completed and returned.

Home

R 3-32-2-1 Preston County Board of Education Responsibilities

Pursuant to SBP 2460, Preston 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 Preston 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:

- Electronic storage of educational material should comply with local guidelines and section 4.4.a.6 of SBP 2460.
- The district shall, whenever possible, make available facilities and technology to accommodate distance learning and access to virtual courses provided through the West Virginia Virtual School or approved course providers.
- The district may 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 and network security best practices.

- The district shall provide professional development in the use of technology and its application in the teaching and learning process.
- The district 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 district 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 WVDE strongly recommends student and teacher Acceptable Use Policies be reviewed and accepted annually by users and/or guardians.
- The district 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, districts 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. The role of the TSS is to manage/repair school local area networks and connected devices. Employment of adequate technology personnel at each school is important to ensure the safety of students and acceptable use of electronic resources, technologies, and the Internet; to implement school policies through technology integration/fluency; and to manage/repair school local area networks, software and hardware.
- The use and administration of a network server for Internet connection within the district 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, including but not limited to service patches, updates, and malware detection software, to the server are the responsibility of the designated/approved educator/net administrator serving that location.
- All remote access to servers located within the district 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 support only the e-mail accounts administered by the WVDE and approved provider(s). E-mail accounts not provided or approved by the WVBE should not be used for school/educational purposes. All liability for any email accounts not provided or approved by the WVBE 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.
- Districts, schools, educators and staff may publish student pictures, video image student pictures or names on class, school or district web sites and social media only when such elements are designated by district policy as directory information in accordance with FERPA and {policy 4350. Parental consent/permission should be obtained (e.g. through photo release forms). Schools and districts should develop local policies regarding online publishing of student information that applies to staff, students, and volunteers. (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 WVDE provides protective measures for filtering of Internet access to content that is: (a) obscene; (b) child pornography; or (c) harmful to minors. Districts may choose to provide additional levels of protection.

- Districts and schools are subject to CIPA and are required to adopt and implement an Internet Safety Policy addressing: pursuant to federal law (47 U.S.C. 254).
- Before adopting an Internet safety policy, districts and schools must provide reasonable notice and hold at least one public hearing or meeting to address the acceptable use policy.
- District Internet Safety Policies must include the monitoring and filtering of the online activities of students all users. Internet safety policies must provide for educating all users about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. Pursuant to section 5.4.g of SBP 2460, WVBE will provide guidance for such activities.
- Preston 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. School districts may permit the use of personal devices (cell phones, smart phones, tablets, digital cameras, etc.) pursuant to local policies and guidelines. 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 unapproved personal devices during class.
  - 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.
- Preston County Schools will provide professional development and classroom lessons regarding the compliance with copyright laws.
- Preston 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.

R 3-32-2-2 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 Preston 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:

- To the extent practicable and as funds and other resources are available, schools should foster the use 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 and network security best practices .
- Every school shall have a school technology team and a comprehensive technology plan. Schools may choose to have the local School Improvement Council, the faculty senate or the curriculum team may serve as the technology team.
- Schools must follow the guidelines of CIPA and the Children's Online Privacy Protection (COPPA) federal statutes.
- Schools shall provide the necessary professional development to enable teachers to incorporate technology into the classroom.

- 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 Internet provided by the school, district, 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
- See also school responsibilities that may be listed in association with county boards of education and district responsibilities *(R 3-32-2-1)* and educator, service personnel and staff responsibilities (*R 3-32-2-3*).

Home

R 3-32-2-3 Educator, Service Personnel and Staff Responsibilities

All educators, service personnel, and staff are expected to maintain appropriate boundaries between personal social networking and professional/educational networking to protect the safety of the students and professional integrity. For the protection of students and employees, it is recommended that any adult communication with students occur either via one-way communication applications or district sponsored applications, or that communication occur directly with parents. District policies may specifically designate the methods of electronic communication that are acceptable for use by educators, service personnel and staff to use when communication with students is necessary.

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 adults who have contact with students due to their work on behalf of an education agency. Failure to adhere to these regulations may result in disciplinary action and/or loss of licensure:

- Adults 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 provided computer or other work provided 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.

Educators will promote and model acceptable use, digital citizenship and online responsibility to support personalized learning and digital-age assessments to meet applicable educational learning policies, 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 shall not use copyrighted material in a manner that violates copyright law or is contrary to terms of use provided by the owner of the materials. WVDE assumes no liability for local violations of 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

R 3-32-3 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 access privileges.
- 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 district/school.
- School personnel shall also receive acceptable use training.
- It is the expectation for all Preston County School employees to be provided with a K-12 email account, and all professional correspondence should be completed using this assigned K-12 email account.
- It is the expectation for all Preston County School employees to be provided with a K-12 email account, and all professional correspondence should be completed using this assigned K-12 email account.
- 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; 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 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 or equipment. The WVDE reserves the right to disclose any electronic message, files, media, and other information 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. Based upon the acceptable use and safety guidelines outlined in this document, WVDE, State Superintendent of Schools and WVDE system administrators will determine what appropriate use is, and their decision is final.
- Violation of use policies could result in loss of access, personal payment of fees incurred, employment discipline, licensure revocation and/or prosecution. Other consequences for students may be found in Policy 4373.
- Administrative information systems, including WVEIS, are to be used exclusively for educational purposes. Ownership of student, personnel, and financial records remains with the agency with primary responsibility for maintenance of the information. WVDE reserves the right to access data maintained in or transmitted over state supported information systems and disclose it as appropriate for legitimate purposes. All staff must maintain the confidentiality of student data in accordance with FERPA and Policy 4350.
- These guidelines may be superseded by FERPA and other appropriate federal and state laws to the extent that such laws are more restrictive.

Home

R 3-32-4 Internet and Telecommunication Acceptable Use Procedures

The Preston 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

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 technology 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, district, and school to implement the intent of CIPA, COPPA, E-rate guidelines, FERPA, and any other applicable state and federal statute and policy including but not limited to *SBP 4373* and WVC §18-2C-3.) .
.
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;
- The online publication of educational material for instructional purposes and, with parental permission, student work. As required by copyright law, external sources must be cited.
- 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

R 3-32-4-1 Internet and Telecommunications Student Access Consent and Waiver Form

---

Agreement and Parent Permission Form

After reading the attached summary of Preston County Schools policies, please complete this form to indicate that you agree with the terms and conditions of those policies. 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 Preston County Board of Education policies and *SBP 2460 Educational Purposes and Acceptable use of Electronic Resources, Technologies and the Internet.*

School Name_____

STUDENT SECTION

I have read the attached summary of Preston County Schools 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.

Student Name (please print)_____ Grade: _____

Student's Signature: _____ Date: _____

PARENT SECTION

I have read the attached summary of Preston County Schools policies the policies for 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_____

SCHOOL INTERNET WEB STIE STUDENT INFORMATION

I hereby give my permission to use the following information on the school web site. Initial all that you approve.

_____ Student's first name _____ Student's photo

_____ Student in group photo

PLEASE INITIAL IF YOU DO NOT AUTHORIZE ANY PHOTOS OR NAME INFORMATION ON THE SCHOOL WEBSITE: _____

This form will be kept in the school listed above. It will not be transferred to another school. Please read the attached summary of Preston County Schools policies. The span of this agreement will be from the signature date until September 1, 2019

R 3-32-4-2 Internet and Telecommunications Adult Access Consent and Waiver Form

ADULT ACCEPTABLE USE POLICY AGREEMENT

School/Location:_____

After reading the attached Preston County Schools policies, please complete this form 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 Preston County Board of Education policies and SBP 2460.

ADULT 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)_____

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.prestonboe.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:**_____

Please return this form to your building administrator or his/her designee.

Staff members who do not return this form cannot be issued a Password for Internet and Telecommunications access

Home

R 3-32-4-3

PRESTON COUNTY SCHOOLS
NETWORK AND INTERNET ACCEPTABLE USE POLICY (AUP)
TO BE ATTCHED TO ACCEPTABLE USE POLICY AGREEMENTS

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.

The Preston 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 Preston 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 Preston County Schools:

- 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.
- 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 become proficient in college- and career-readiness standards to succeed and prosper in life, in school, and on the job.
- 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.
- To promote student learning, teachers 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.
- The state, districts, and schools will use electronic resources as a powerful and compelling means for students to learn core and elective subjects and applied skills in relevant and rigorous ways to advance learning as referenced in W. Va. Code §18-2e-7, W. Va. 126CSR44N, WVBE Policy 2520.14, West Virginia College- and Career-Readiness Standards for Technology and Computer Science (Policy 2520.14), W. Va. 126CSR42, WVBE Policy 2510, Assuring the Quality of Education: Regulations for Education Programs, and W. Va. 126CSR44A et ~~al~~ seq., WVBE Policy 2520 series.
- 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 quality virtual courses and online educational tools and resources.
- Teachers should integrate high quality digital content and assessment resources with curriculum to personalize learning.
- 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 both provide a safe digital environment, and meet **Federal Communications Commission** (FCC) guidelines and E-rate audits.

R 3-32-1 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/Network Code of Conduct

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, videos, social media, other digital communication platforms, 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.
- Electronic educational material containing confidential student information shall be stored only in secure locations consistent with federal, state, and local privacy regulations. Electronic educational material containing no confidential student information, including but not limited to, lesson plans, worksheets, primary source documents, and other materials used for instruction, may be stored in appropriate locations but should follow state/district guidelines.
- Educators electing to use third party classroom based applications should carefully review the terms of service and privacy policies prior to use for those applications to ensure consistency with best practice. For use of applications with students younger than 13 years of age, recommended best practice is to obtain parental consent prior to use and/or entering any student data. All use of third party applications must be consistent with local policy/guidelines, Family Educational Rights and Privacy Act (20 U.S.C. §1232g; 34 CFR Part 99) FERPA), W. Va. Code §18-2-5h, and W. Va. 126SR94, WVBE
- 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.
- Appropriate permission shall be obtained prior to publishing student pictures or names on class, school, or district web sites or other publications, provided that such information is not designated as directory information under district policy. All releases of information designated as directory information under district policy must comply with parental opt-out provisions as described in the FERPA and WVBE Policy 4350. (Also see *File: 11-19. Collection, Maintenance and Disclosure of Student Data)*
- 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 users other than school, district and/or state officials responsible for implementing the privacy incident response protocol
- 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 may result in revocation of user privileges based on state, district 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.

R 3-32-2 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 File: R 3-32-4 -2 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 and appropriate uses of online resources, technologies and the Internet is a responsibility of all educational staff and employees.

Adult use of Internet-related or web-based applications must be authorized through the *R 3-32-4-2 Internet and Telecommunications Access Consent and Waiver Form*. Access Passwords cannot be issued to adult users until this form is completed and returned.

R 3-32-3 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 access privileges...
- 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 district/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. 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 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 or equipment. The WVDE reserves the right to disclose any electronic message, files, media, and other information, 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. Based upon the acceptable use and safety guidelines outlined in this document, WVDE, State Superintendent of Schools and WVDE system administrators will determine what appropriate use is, and their decision is final.
- Violation of use policies could result in loss of access, personal payment of fees incurred, employment discipline, licensure revocation and/or prosecution. Other consequences for students may ~~also~~ be found in Policy 4373.

- 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.*
- Administrative information systems, including WVEIS, are to be used exclusively for educational purposes. Ownership of student, personnel, and financial records remains with the agency with primary responsibility for maintenance of the information. WVDE reserves the rights to access data maintained in or transmitted over state supported information systems and disclose it as appropriate for legitimate purposes. All staff must maintain the confidentiality of student data in accordance with FERPA and Policy 4350.
- 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.
- These guidelines may be superseded by FERPA and other appropriate federal and state laws to the extent that such laws are more restrictive.

R 32-3-4 Internet and Telecommunication Acceptable Use Procedures

The Preston 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 comply 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, and various media products using network resources in support of student personalized academic learning and educational administration;
- Appropriate participation in school-sponsored sites and online groups;
- The online publication of educational material for instructional purposes and, with parental permission, student work. As required by copyright law, external sources must be cited.
- Incidental personal use in accordance with all district/school policies and guidelines.

R 32-3-5 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:

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

- Inappropriate use or transmission of any material in violation of any federal or state law or regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening, abusive, or obscene material, or material protected by trade secrets.
- 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.
- 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, SPAM, and changes to tools used to filter content or monitor hardware and software.
- 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.
- Using e-mail and other electronic user identifications (IDs)/passwords other than one's own or for unauthorized purposes. Students and staff are responsible for all activity on their account and must not share their account IDs and passwords.
- Supplying your password to others.
- 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 measures when using any form of electronic communications.
- Hacking, cracking, vandalizing or any other unlawful online activities.
- Disclosing, using, or disseminating personal information regarding students.
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks and other unauthorized uses as referenced in, including but not limited to, Policy 4373 and other applicable federal and state statutes.
- Personal gain, commercial solicitation and compensation of any kind.
- Any activity which results in liability or cost incurred by the district.
- Unauthorized downloading, copying, installing and/or executing gaming, audio files, video files or other applications (including shareware or freeware).
- Campaigning, lobbying, or other activity via state supported platforms in support or opposition for political activity or issues, including but not limited to, ballot measures, candidates, or legislative proposals.
- Information posting, sending or storing information that could endanger others.
- Engaging in plagiarism or reproducing or repurposing media without permission.
- Attaching unauthorized equipment to the district or school networks or network connect devices. 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 including but is not limited to, uploading, downloading, or creating computer viruses or malware. Vandalism may result in revocation of user privileges and/or prosecution.
- Uses related to or in support of illegal activities will be reported to authorities.
- It is unacceptable to give administrative responsibilities for a server with a wide area network or Internet connection to a current PreK-12 student outside of a laboratory environment, as with career and technical education computer related courses.

Home

R 3-32-5 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 federal or state law **or** regulation, 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:

- Inappropriate use or transmission of any material in violation of any federal or state law or regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening, abusive, or obscene material, or material protected by trade secrets.
- 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.
- 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 identifications (IDs)/passwords other than one's own or for unauthorized 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 to others.
- 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 any form of electronic communications.
- Hacking, cracking, vandalizing or any other unlawful online activities.
- Disclosing, using, or disseminating personal information regarding students.
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks and other unauthorized uses as referenced in, but not limited to, Policy 4373 and other applicable federal and state statutes.
- Personal gain, commercial solicitation and compensation of any kind.
- Any activity which results in liability or cost incurred by the district.
- Unauthorized downloading, copying, installing and/or executing gaming, audio files, video files or other applications (including shareware or freeware).
- Campaigning, lobbying, or other activity via state supported platforms in support or opposition for political activity or issues, including but not limited to, ballot measures, candidates, or legislative proposals.
- Engaging in plagiarism or reproducing/repurposing media without permission.
- Information posted, sent or stored online that could endanger others.

- 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 including but is not limited to, uploading, downloading, or creating computer viruses or malware. Vandalism may result in revocation of user privileges and/or prosecution.
- It is unacceptable to give administrative responsibilities for a server with a wide area network or Internet connection to a current PreK-12 student outside of a laboratory environment, as with career and technical education computer related courses.

R 3-32-6 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 and any other equipment which communicates via network connections.

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.

Home

R 3-32-7 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. Violation of copyright laws may expose the user, district, or school to legal action and/or financial penalties.

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. Consult the Fair Use Doctrine of the United States Copyright Act, (17 U.S.C. §101-810), for guidance about using such material in an educational context.

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.
- Unauthorized duplication of copyrighted material and/or use of such unauthorized material on state, district, or school equipment or networks is prohibited
- 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 user agreements including, but not limited to, terms and conditions, terms of use, End User License Agreements (EULA), and copyright prior to utilizing content from resources and software licenses to ensure compliance with the terms of the user agreements.

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

R 3-32-8 Web Publishing

The Preston 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" Preston 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
  - 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.
  - Remain current, be accurate, and incorporate easy and user-friendly 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/distdrict. 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.
- Complies with all W3C and ADA standards

✣ Consult the World Wide Web Consortium (W3C) for additional web publishing standards including accessibility guidelines.

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

Amended/Revised: February10, 2014; July 24, 2017

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 Preston 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 Preston 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 Preston 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 available to them. 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 Common Sense Media. 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 Preston 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.

Preston 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.

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.

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: