TITLE 126
LEGISLATIVE RULE
BOARD OF EDUCATION

SERIES 41
EDUCATIONAL PURPOSE AND ACCEPTABLE USE OF ELECTRONIC RESOURCES, TECHNOLOGIES AND THE INTERNET (2460)

§126-41-1. General.

1.1. Scope. – W. Va. 126CSR41, West Virginia Board of Education (WVBE) Policy 2460, *Educational Purpose and Acceptable Use of Electronic Resources, Technologies and the Internet* (Policy 2460)**,** is a policy name change and the replacement of the repealed policies noted in section 1.5 to: 1) include the new federal regulations regarding issues of child safety and acceptable use of the Internet; 2) be in compliance with Universal Service Fund for Schools and Libraries (E-rate) guidelines; 3) reinforce copyright compliance; and 4) align with other federal and state regulations.

1.2. Authority. – W. Va. Constitution, Article XII, Section 2 and W. Va. Code §18-2-5.

1.3. Filing Date. – March 16, 2012

1.4. Effective Date. – April 16, 2012

1.5. Repeal of former rule. - This legislative rule repeals and replaces W. Va. §126CSR41, "Use of Internet by Students and Educators" (Policy 2460) filed August 10, 2001, and effective September 9, 2001; and repeals W. Va. §126CSR43, "Use of Technology by Students and Educators" (Policy 2470) filed December 15, 1996, and effective July 1, 1997, and W. Va. §126CSR153, "Copyright Protected Computer Software, Print and Non-Print Media" (Policy 5711) filed December 22, 1992, and effective January 23, 1993.

§126-41-2. Purpose.

2.1. Policy 2460 sets out regulations that apply to districts (counties), schools, students, educators, other school personnel, parents, guardians, county boards of education, Regional Education Service Agencies (RESAs), West Virginia Department of Education (WVDE) and other users.

2.2. These regulations will assist implementation of policies at the state, RESA, district, and school levels 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.

§126-41-3. Educational Purposes.

3.1. 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.

3.2. 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.

3.3. 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.

3.4. 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.

3.5. 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, 21st Century Learning Skills and Technology Tools Content Standards and Objectives for West Virginia Schools (Policy 2520.14), W. Va. 126CSR42, WVBE Policy 2510, Assuring the Quality of Education: Regulations for Education Programs, and W. Va. 126CSR44A et al., WVBE Policy 2520 et al., 21st Century/Next Generation Standards.

3.6. 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.

3.7. 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.

3.8. Teachers 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.

3.9. 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.

3.10. 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. (See links at http://wvde.state.wv.us/technology/policy2460.php.)

3.11. Districts should adopt local policies which outline consequences for safety and acceptable use in alignment with federal and state laws, state and district policies, especially W. Va. 126CSR99, WVBE Policy 4373, Expected Behavior in Safe and Supportive Schools (Policy 4373).

§126-41-4. Digital Citizenship.

4.1. The appropriate use of technology and digital resources promotes positive and effective digital citizenship among students and staff. 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.

4.2. All users need to be part of this digital citizenry to appropriately and safely learn, work, play, and live in today's global society.

4.3. The International Society for Technology in Education (ISTE) has produced materials in the book, *"Digital Citizenship in Schools"* that describes nine elements of digital citizenship.

4.3.a Digital Access - full electronic participation in society.

4.3.b. Digital Commerce - the buying and selling of goods online.

4.3.c. Digital Communication - the electronic exchange of information.

4.3.d. Digital Literacy - the capability to use digital technology and knowing when and how to use it.

4.3.e. Digital Etiquette - the standards of conduct expected by other digital technology users.

4.3.f. Digital Law - the legal rights and restrictions governing technology use.

4.3.g. Digital Rights and Responsibilities - the privileges and freedoms extended to all digital technology users, and the behavioral expectations the come with them.

4.3.h. Digital Health and Wellness - the elements of physical and psychological well-being related to digital technology use.

4.3.i. Digital Security - the precautions that all technology users must take to guarantee their personal safety and the security of their networks.

4.4. Digital/Network Etiquette:

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

4.4.a.1. Be polite. Do not write or send abusive messages to others.

4.4.a.2. Use proper English and appropriate language; avoid "Netspeak." Do not swear; do not use vulgarities or other inappropriate language.

4.4.a.3 Use extreme caution when revealing personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.

4.4.a.4. Do not reveal, on any electronic medium, personal information about another individual.

4.4.a.5. 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).

4.4.a.6. Keep educational files and e-mail messages stored on servers to a minimum. (Also see section 5.6.v.)

4.4.a.7. Activate the appropriate automatic reply message and unsubscribe to listservs if account is to be unused for an extended period of time.

4.4.a.8. 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 W. Va. 126CSR94, WVBE Policy 4350, Procedures for the Collection, Maintenance and Disclosure of Student Data.)

4.4.a.9. Notify the appropriate school authority of any dangerous or inappropriate information or messages encountered.

4.5. Digital Security:

4.5.a. Users who identify a security problem on the system must notify a system administrator.

4.5.b. Users must not demonstrate the problem to other users.

4.5.c. 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.

4.5.d. 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. (See also section 5.6.i.)

4.5.e. 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.

§126-41-5. Accountability and Responsibility.

5.1. 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. (W. Va. Code § 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 a county-determined procedure. 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.

5.2. The following statements delineate the responsibilities of the WVBE, WVDE, RESAs, county boards of education, individual schools, educators and other educational/service personnel for the appropriate and authorized use of technologies, digital resources and the Internet.

5.3. WVBE responsibilities, based on authority of W. Va. Code, will include approving policies advocating the following activities:

5.3.a. Students will be provided equitable access to technology.

5.3.b. Students will graduate from the public schools with proficiency in the skills and learning objectives delineated in instructional policies, especially in Policy 2520.14.

5.3.c. Policy 2520.14 content standards and objectives will be included as part of the instructional goals and objectives of all programs of study and at all grade levels.

5.3.d. The WVBE will collaborate with the higher education community to communicate complementary technology utilization initiatives and partnerships and readiness of student teachers in understanding the professional role of the educator and the position of trust.

5.3.e. Administrators and teachers will be provided professional development in the use and application of electronic resources, technologies and the Internet.

5.4. WVDE responsibilities will include carrying out the policies of the WVBE and include the following tasks/duties:

5.4.a. 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 and goals.

5.4.b. The WVDE reserves the right to monitor, inspect, investigate, copy, review and store, without prior notice, information about the content and usage of any network and system files, user files, disk space utilization, applications, bandwidth utilization, document files, folders, 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.

5.4.c. 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).

5.4.d. The WVDE will review and process appropriate applications for domain names for local servers.

5.4.e. The WVDE reserves the right to disclose any electronic message, files, media, etc., to law enforcement officials or third parties as appropriate.

5.4.f. Based upon the acceptable use and safety guidelines outlined in this document, The State Superintendent of Schools, WVDE and provider(s) system administrators will determine what appropriate use is, and their decision is final.

5.4.g. The WVDE reserves the right to enter an employee's information system files whenever there is a business need to do so.

5.4.h. Electronic filtering will be installed by the WVDE 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/schools to meet Children's Internet Protection Act (CIPA) and E-Rate guideline requirements for filtering.

5.4.i. 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. The districts and schools are encouraged to go beyond this basic compliance if so desired.

5.4.j. The state network will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the state's computer network or the Internet.

5.4.k. The WVDE makes no warranties of any kind, whether expressed or implied, for the service being provided. The WVDE will not be responsible for any damages, including loss of data or service interruptions. The use of any information obtained via the system is at the user's own risk. WVDE is not responsible for the accuracy and quality of information obtained through the system.

5.5. RESA responsibilities include supporting the WVBE and WVDE in carrying out state and federal contracts, policies and legislation relating to electronic resources, technologies and the Internet, such as, but not limited to:

5.5.a. RESAs may support respective counties served in providing professional development to implement Policy 2520.14.

5.5.b. RESAs will provide timely and appropriate repair, telecommunications assistance, West Virginia Education Information System (WVEIS) support and other services addressed in state policies and statutes.

5.6. County boards of education responsibilities:

5.6.a. All county boards shall have a county technology team and a comprehensive technology plan that is included as part of the Five-Year Online Strategic Plan. In addition to the county technology director/contact, the technology team should be representative of areas including instruction, finance, facilities, personnel and others as designated by the county.

5.6.b. Policy 2520.14 shall be included in all programs of study and at all grade levels.

5.6.c. County boards 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.

5.6.d. County boards, 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.

5.6.e. County boards shall provide professional development in the use of technology and its application in the teaching and learning process.

5.6.f. County boards 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.

5.6.g. County boards 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.

5.6.h. In accordance with W. Va. Code, school aid formula and local funding opportunities, county boards 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. It is highly important to have adequate technology personnel at each school to ensure the safety of students and acceptable use of electronic resources, technologies, and the Internet. It is imperative to have adequate technology personnel at the school level to implement school policies through technology integration/fluency by the TIS and manage/repair school local area networks through TSS and to ensure the safety of students and acceptable use of electronic resources, technologies and the Internet.

5.6.i. The use and administration of a network server for Internet connection within a county or school is the responsibility of the designated/approved educator(s) and 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/administrator serving that location.

5.6.j. All remote access to servers located at a county or school building and connected to a wide area network and/or the Internet is the responsibility of the 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.

5.6.k. 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.

5.6.l. 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.k12.wv.us” e-mail accounts should not be used for school/educational purposes. 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.

5.6.m. 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. (See also Policy 4350.) Schools and districts should develop local policies regarding online publishing.

5.6.n. 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.

5.6.o. 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.

5.6.p. 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.

5.6.q. 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 section 5.4.i. for details and http://wvde.state.wv.us/technology/cipa-compliance.htm)

5.6.r. District/school equipment that is used off site is subject to the same rules as when used on site.

5.6.s. 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.

5.6.t. Students and staff are encouraged to use district and school equipment whenever possible. 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:

5.6.t.1. Using personal devices to gain or give an advantage in a testing situation.

5.6.t.2. 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).

5.6.t.3. Downloading and installing district licensed software on personal devices unless specifically allowed by the licensing agreement.

5.6.t.4. Using personal devices to bypass filtering, circumvent network security, or in violation of the acceptable use standards which normally apply to district-owned technology.

5.6.t.5. Using personal devices for violations related to cyber bullying and harassment.

5.6.u. Districts/schools should provide professional development and classroom teaching regarding the compliance of copyright laws. (See also http://wvde.state.wv.us/technology/policy2460.php) and §126-41-9. Copyright.)

5.6.v. Keep educational files and e-mail messages stored on servers to a minimum. Users should responsibly back up their data and files. Counties may set individual storage limits per server.

5.7. School Responsibilities:

5.7.a. 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.

5.7.b. 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 council or the faculty senate or the curriculum team serve as the technology team.

5.7.c. Policy 2520.14 shall be taught and utilized throughout all the programs of study and at all grade levels.

5.7.d. Five-Year Online Strategic Plan will include necessary professional development to enable teachers to incorporate technology into the classroom.

5.7.e. 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.

5.7.f. 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.

5.7.g. Schools must follow the guidelines of CIPA and the Children's Online Privacy Protection federal statutes (COPPA).

5.7.h. See also school responsibilities that may be listed in association with county boards of education and district responsibilities (section 5.6) and educator, service personnel and staff responsibilities (section 5.8).

5.8. Educator, Service Personnel and Staff Responsibilities:

5.8.a. 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.

5.8.b. 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:

5.8.b.1. 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.

5.8.b.2. 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.

5.8.b.3. 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.

5.8.c. 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.

5.8.d. 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.

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

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

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

§126-41-6. Use of Electronic Resources, Technology and the Internet.

6.1. Overview of Use:

6.1.a. 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.

6.1.b. 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.

6.1.c. 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:

6.l.c.1. The network and system files;

6.l.c.2. User files and disk space utilization;

6.l.c.3. User applications and bandwidth utilization;

6.l.c.4. User document files, folders and electronic communications;

6.l.c.5. E-mail;

6.l.c.6. Internet access; and

6.l.c.7. Any and all information transmitted or received in connection with networks, e-mail use and web-based tools.

6.1.d. 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.

6.1.e. 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.

6.1.f. 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 Policy 4373.

6.1.g. 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).

6.1.h. 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.

6.1.i. Any of these guidelines are to be cognizant of and superseded by FERPA and other appropriate federal and state laws.

6.2. Acceptable Use:

6.2.a. 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.

6.2.b. 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.

6.2.c. State, district and school-owned technology is to be used to enhance learning and teaching as well as improve the operation of the district and school.

6.2.d. 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 Policy 4373 and W. Va. Code §18-2C-2.)

6.2.e. Acceptable network use by students and staff includes the following:

6.2.e.1. Creation of files, projects, videos, web pages and podcasts using network resources in support of student personalized academic learning and educational administration;

6.2.e.2. Appropriate participation in school-sponsored blogs, wikis, web 2.0+ tools, social networking sites and online groups;

6.2.e.3. 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;

6.2.e.4. Staff use of the network for incidental personal use in accordance with all district/school policies and guidelines.

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

6.3. Unacceptable Use:

6.3.a. Inappropriate use or transmission of any material in violation of any U.S. 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.

6.3.b. Use for commercial activities by for-profit institutions is not acceptable.

6.3.c. Use for product advertisement or political lobbying is also prohibited.

6.3.d. Illegal activities and privacy and safety violations of COPPA, CIPA and FERPA are strictly prohibited.

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

6.3.e.1. Viewing, creating, accessing, uploading, downloading, storing, sending, or distributing obscene, pornographic or sexually explicit material.

6.3.e.2. Downloading, uploading and/or executing viruses, worms, Trojan horses, time bombs, bots, malware, spyware, SPAM, etc., and changes to tools used to filter content or monitor hardware and software.

6.3.e.3. 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.

6.3.e.4. 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.

6.3.e.5. Supplying your password and user information to any electronic request or sharing them with others via any other communications.

6.3.e.6. Storing passwords in a file without encryption.

6.3.e.7. Using the “remember password” feature of Internet browsers and e-mail clients.

6.3.e.8. Leaving the computer without locking the screen or logging off.

6.3.e.9. Corrupting, destroying, deleting, or manipulating system data with malicious intent.

6.3.e.10. Requesting that inappropriate material be transferred.

6.3.e.11. 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.

6.3.e.12. Hacking, cracking, vandalizing or any other unlawful online activities.

6.3.e.13. Disclosing, using, or disseminating personal information regarding students.

6.3.e.14. 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.

6.3.e.15. Personal gain, commercial solicitation and compensation of any kind.

6.3.e.16. Any activity which results in liability or cost incurred by the district.

6.3.e.17. Downloading, installing and/or executing non-educational gaming, audio files, video files or other applications (including shareware or freeware) without permission or approval.

6.3.e.18. Support or opposition for ballot measures, candidates and any other political activity.

6.3.e.19. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture, etc.).

6.3.e.20. Plagiarism or reproducing/repurposing audio/video without permission/consent.

6.3.e.21. 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 W. Va. Code §61-3C-5, Unauthorized Access To Computer Services.

6.3.e.22. 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.

6.3.e.23. 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.

6.3.e.24. Uses related to or in support of illegal activities will be reported to authorities.

§126-41-7. Network.

7.1. 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.

7.2. 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.

7.3. 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.

7.4. 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.

7.5. 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.

7.6. 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.

7.7. 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.htm. This WVDE method will provide documentation that districts have met the annual E-rate compliance requirements of educating students regarding appropriate use.

§126-41-8. Filtering.

8.1. 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.

8.2. 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.

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

8.4. 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.

8.5. 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.

8.6. Appropriate filtering must be maintained to meet E-rate guidelines. (See also section 7.5.)

§126-41-9. Copyright.

9.1. 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.

9.2. 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/title17) and content is cited appropriately.

9.3. 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:

9.3.a. The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes.

9.3.b. The nature of the copyrighted work.

9.3.c. The amount and substantiality of the portion used in relation to the copyrighted work as a whole.

9.3.d. The effect of the use upon the potential market for, or value of, the copyrighted work.

9.4. To discourage violation of copyright laws, the following compliance requirements are specified:

9.4.a. Employees and students are expected to adhere to the copyright laws.

9.4.b. Appropriate software licenses will be obtained for use in a network server system or other multi-access use.

9.4.c. Programs available through the statewide provisions of technology implementation must comply with stipulations of the various purchase agreements.

9.4.d. Illegal copies of copyrighted programs shall not be made or used on state, RESA, district or school equipment. (See also section 9.2.)

9.4.e. Students are to be taught the ethical and practical problems and consequences of plagiarism and software/media piracy.

9.4.f. 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.

9.4.g. 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.)

9.5. 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 W. Va. Code §18A-2-8.

§126-41-10. Web Publishing.

10.1. The WVDE recognizes the educational benefits of publishing information on the Internet by school personnel and students. The WVDE 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 WVDE recommends that each county and/or school adopt local policies that are consistent with, but not limited to, the following web publishing guidelines:

10.1.a. The "official" district/school web site may be administered by the district/school designated authority.

10.1.b. 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.

10.1.c. 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.

10.2. Web site content should:

10.2.a. Be appropriate, in good taste, and not harmful to any individual or group.

10.2.b. Be grammatically correct, accurately spelled, and have a pleasing appearance.

10.2.c. 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.

10.2.d. Comply with WVBE policies and regulations.

10.2.e. Include information such as an e-mail address of the responsible contact person, copyright, and the last date updated should be included.

10.2.f. Remain current, be accurate, and navigation through the site should be easy and user friendly.

10.2.g. 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.

10.2.h. Comply with copyright, intellectual property, state, federal (specifically COPPA and CIPA) and international law.

10.2.i. Include the permission granted statement (who, time period, etc.) for all copyrighted materials.

10.3. Consult the World Wide Web Consortium (W3C) for additional web publishing standards at http://www.w3.org/standards/webdesign.

10.4. The W3C Web Accessibility Initiative (WAI) develops Web accessibility guidelines. More information is available at http://www.w3.org/WAI/intro/components.php.

§126-41-11. Implementation.

11.1. County Boards of Education:

11.1.a. County boards of education will ensure implementation of this policy by adopting their own county/school policies regarding acceptable use of electronic resources, technologies and the Internet.

11.2. WVDE:

11.2.a. The WVDE shall provide technical assistance to support RESAs, counties, and schools in developing and implementing local use policies. RESAs may also provide professional development support to counties and schools in addressing acceptable use.

11.2.b. The WVDE shall assist counties and schools with revisions of the Five-Year Online Strategic Plans associated with technology implementation and the West Virginia State Technology Plan.

§126-41-12. Incorporation by Reference.

12.1. A copy of the West Virginia Educational Technology Plan is incorporated by reference and may be reviewed at http://wvde.state.wv.us/technology/techplan/index.php.

12.2. E-rate Compliances. A list of E-rate compliances will be provided at http://wvde.state.wv.us/technology.

12.3. Guidance procedures to address definitions, technological changes, best practices and FAQs. See: http://wvde.state.wv.us/technology/policy2460.php.

§126-41-13. Severability.

13.1. If any provision of this rule or the application thereof to any person or circumstance is held invalid, such invalidity shall not affect other provisions or applications of this rule.