WEST VIRGINIA SECRETARY OF STATE

MAC WARNER

ADMINISTRATIVE LAW DIVISION

eFILED

1/11/2018 10:29 AM

NOTICE OF FINAL FILING AND ADOPTION OF A LEGISLATIVE EXEMPT, INTERPRETIVE OR PROCEDURAL RULE

AGENCY: Education

TITLE-SERIES: 126-041

RULE TYPE: Legislative Exempt

Amendment to Existing Rule: Yes

Repeal of existing rule: No

RULE NAME: Educational Purpose and Acceptable Use of Electronic Resources, Technologies and the Internet (2460)

CITE STATUTORY AUTHORITY: W. Va. Code §§29A-3B-1, et seq.; W. Va. Board of Education v. Hechler, 180 W. Va. 451; 376 S.E.2d 839 (1988)

This rule is filed with the Secretary of State. This rule becomes effective on the following date:

July 1, 2018

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. -- This legislative rule establishes the educational purpose and acceptable use of electronic resources, technologies and the Internet. This policy applies to all West Virginia school districts. Districts include county boards of education, the West Virginia School for the Deaf and Blind, the Office of Diversion and Transition Programs, and any other schools under the supervision of the West Virginia Board of Education (WVBE) and West Virginia Department of Education (WVDE). The guidelines set forth in this policy apply to any individual using a state, district, or school provided electronic device or network, regardless of whether the individual is on or off of state, district, or school property and regardless of whether the activity takes place during the individual's normal work hours.

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

1.3. Filing Date. -- January 11, 2018.

1.4. Effective Date. -- July 1, 2018.

1.5. Repeal of Former Rule. -- This legislative amends W. Va. §126CSR41, Educational Purpose and Acceptable Use of Electronic Resources, Technologies and the Internet (Policy 2460), filed March 16, 2012, and effective April 16, 2012.

§126-41-2. Purpose.

2.1. 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.

2.2. These regulations will assist implementation of policies at the state, 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 become proficient in college- and career-readiness standards 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, 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.

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 quality virtual courses and online educational tools and resources.

3.8. Teachers should integrate high quality digital content and assessment resources with curriculum to personalize learning.

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 both provide a safe digital environment, and meet Federal Communications Commission (FCC) guidelines and E-rate audits.

3.11. Districts should adopt local policies which outline consequences for violation of safety and acceptable use in alignment with federal and state laws, state and district policies, specifically 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) includes standards and provides guidance related to digital citizenship for students, teachers, administrators, instructional coaches and computer science educators.

4.4. Digital/Network Code of Conduct:

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, videos, social media, other digital communication platforms, 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.

4.4.a.6. 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.

4.4.a.7. 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 Policy 4350, Procedures for the Collection, Maintenance and Disclosure of Student Data (Policy 4350).

4.4.a.8 Activate the appropriate automatic reply message if account is to be unused for an extended period of time.

4.4.a.9. 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.

4.4.a.10. 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. 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.

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

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 may result in revocation of user privileges based on state, district, or school policies.

4.5.d. Any user identified as a security risk may be denied access by the appropriate disciplinary authority.

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 district determined procedure. 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.

5.2. The following statements delineate the responsibilities of the WVBE, WVDE, districts, 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 standards delineated in instructional policies.

5.3.c. Policy 2520.14 content standards will be included as part of the instructional goals of all programs of study and at all grade levels, K-12.

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

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 providers will support local, state, and federal investigations as required by law. The WVDE reserves the right to disclose any electronic message, files, media, etc., to law enforcement officials or third parties as appropriate.

5.4.d. The State Superintendent of Schools, WVDE staff, and district staff system administrators, using this document as a guide, are the final arbiters of acceptable and safe use of electronic resources, technologies, and the Internet.

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

5.4.f. 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.g. The WVDE will provide guidance and support for appropriate instruction by which districts/schools ~~to~~ certify compliance with current Federal Communications Commission (FCC) regulations regarding Internet safety policies. Districts must provide for educating students about appropriate online behavior, including digital citizenship, interacting with other individuals on social networking websites and other digital communication platforms rooms, and cyber bullying awareness and response. Further, the WVDE will provide support for certifying that students have been educated about appropriate online behavior as well as support federal reporting when districts provide evidence they 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.

5.4.h. The WVDE 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.i. 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.

5.4.j. The WVDE will provide appropriate telecommunications assistance, West Virginia Education Information System (WVEIS) support and other services addressed in state policies and statutes.

5.5. District responsibilities:

5.5.a. All districts shall have a district technology team and an annual comprehensive strategic technology plan. In addition to the district technology director/contact, it is recommended the technology team include representatives from areas of instruction, finance, facilities, personnel and others as designated by the district.

5.5.b. Electronic storage of educational material should comply with local guidelines and section 4.4.a.6 of this procedure.

5.5.c. Districts shall, whenever possible, make available facilities and technology to accommodate distance learning and access to virtual courses provided through the West Virginia Virtual School (WVVS) or approved course providers.

5.5.d. Districts 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.

5.5.e. Districts shall provide professional development in the use of technology and its application in the teaching and learning process.

5.5.f. Districts shall implement appropriate policies to help ensure the safety of the students and acceptable use of electronic resources, technologies and the Internet. Districts 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.

5.5.g. Districts shall provide adequate technology personnel to implement appropriate policies and manage district/school networks to help ensure the safety of students and acceptable use of electronic resources, technologies and the Internet.

5.5.h. 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.

5.5.i. The use and administration of a network server for Internet connection within a district 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, including but not limited to service patches, updates, and malware detection software, to the server are the responsibility of the designated/approved educator/administrator serving that location.

5.5.j. All remote access to servers located at a district 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, remote access to servers must be in accordance with federal, state and local guidelines for appropriate Internet access.

5.5.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.

5.5.l. 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 WVDE should not be used for school/educational purposes. All liability for e-mail accounts not provided or approved by the WVDE 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.

5.5.m. Districts, schools, educators, and staff may publish student pictures, video images 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.

5.5.n. Districts and schools subject to CIPA may not receive ~~the~~ E-rate discounts without certifying 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.

5.5.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.

5.5.p. Districts and schools are subject to CIPA and are required to adopt and implement an Internet safety policy pursuant to federal law (47 U.S.C. 254).

5.5.q. District Internet safety policies must include the monitoring and filtering of the online activities of 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. WVDE will provide guidance for such activities.

5.5.r. District/school equipment is subject to existing rules and policies whether onsite or offsite.

5.5.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.

5.5.t. Students and staff are encouraged to use district and school equipment whenever possible. Districts may permit the use of personal devices (e.g. cell phones, smart phones, tablets, digital cameras, MP3 players, and laptops) pursuant to local policies and guidelines. Unauthorized or unacceptable use of personal technology devices may result in suspension or revocation of personal device privileges. These uses include, but are not limited to, the following:

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

5.5.t.2. Using unapproved personal devices during class.

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

5.5.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.

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

5.5.u. Districts/schools should provide professional development for staff and classroom instruction for students regarding the compliance of copyright laws. (See §126-41-9 of this procedure.)

5.6. School responsibilities:

5.6.a. 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.

5.6.b. Every school shall have a school technology team and a comprehensive technology plan. Schools may choose to have the Local School Improvement Council (LSIC), the faculty senate, or the curriculum team serve as the technology team.

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

5.6.d. Schools shall provide the necessary professional development to enable teachers to incorporate technology into the classroom.

5.6.e. It is the responsibility of the student, parent, teacher, and administrator to follow acceptable use policies, as well as state and federal laws, so that access to telecommunication networks, computers and the Internet provided by the school, district, and state educational systems is not abused.

5.6.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 is required of all wireless access points.

5.7. Educator, service personnel and staff responsibilities:

5.7.a. 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.

5.7.b. In order to assist in maintaining ~~a~~ professional relationships with students and to avoid situations that could lead to inappropriate relationships between adults 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:

5.7.b.1. Adults will maintain ~~a~~ professional, ethical relationships with all 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 behaviour that constitutes a violation of district or county policy or that is detrimental to the health and welfare of students.

5.7.b.2. The viewing, storing, transmitting, 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 or service, 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.

5.7.b.3. All information stored within work computers or servers is the property of the state, district or school, and the personnel using such computers/servers/networks have no expectation of privacy with respect to its contents.

5.7.c. 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.

5.7.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.

5.7.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 §49-2-803, must report as law requires.

5.7.f. Staff members shall not use materials in violation of copyright law or contrary to terms of use provided by the owner of the materials. WVDE assumes no liability for local violations of copyright law.

5.7.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, unacceptable, or unsafe use of the Internet as part of an educational program by students, educators or staff may result in suspension or revocation of ~~such~~ use access privileges.

6.1.b. Each student accessing 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.

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. Users have no expectation of privacy. 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.

6.1.d. 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.

6.1.e. No temporary accounts will be issued, nor will ~~a~~ student or staff use an Internet account not specifically created for him or her. Based upon the acceptable use and safety guidelines outlined in this document, the WVDE, State Superintendent of Schools, and WVDE system administrators will determine what is appropriate use ~~is~~, and their decision is final.

6.1.f. 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.

6.1.g. 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.

6.1.h. Employees may not attempt to gain access to another employee's files in the WVDE's information systems. The WVDE reserves the right to enter an employee's information system files whenever there is a legitimate need to do so.

6.1.i. These guidelines may be superseded by FERPA and other appropriate federal and state laws to the extent that such laws are more restrictive.

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 comply with the rules and regulations of the network provider(s) serving West Virginia districts 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, 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 Policy 4373 and W. Va. Code §18-2C-3.

6.2.e. Acceptable network use by students and staff includes, but may not be limited to the following:

6.2.e.1. Creation of files, projects, and various media products using network resources in support of student personalized learning and educational administration.

6.2.e.2. Appropriate participation in school-sponsored sites and online groups.

6.2.e.3. 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.

6.2.e.4. Incidental personal use by staff not contrary to district/school policies and guidelines.

6.3. Unacceptable Use:

6.3.a. 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.

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, and changes to tools used to filter content or monitor hardware and software.

6.3.e.3. 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.

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 to others.

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 any form 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, sending 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.

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

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

6.3.e.17. Unauthorized downloading, copying, installing and/or executing gaming, audio files, video files or other applications (including shareware or freeware).

6.3.e.18. 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.

6.3.e.19. Posting, sending, or storing information that could threaten or endanger others.

6.3.e.20. Engaging in plagiarism or reproducing/repurposing media without permission.

6.3.e.21. Attaching unauthorized equipment to the district or school networks or network connected devices. Any such equipment may be confiscated and/or turned over to law enforcement officers for potentially violating W. Va. Code §61-3C-5.

6.3.e.22. Attaching unauthorized equipment or making unauthorized changes to the state backbone network. Unauthorized equipment may be confiscated and/or turned over to law enforcement officers for potentially violating W. Va. Code §-61-3C-5. Only WVDE network personnel may authorize changes affecting the state backbone network.

6.3.e.23. 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.

6.3.e.24. Uses related to or in support of illegal activities.

6.3.e.25. Provision of 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.

§126-41-7. Network.

7.1. The statewide network, the district 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.

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 federal and state statutes.

7.4. WVDE, approved service providers, and other state agencies operate the statewide infrastructure to provide Internet access for all schools under the supervision 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 current FCC regulations regarding Internet safety policies.

§126-41-8. Filtering.

8.1. Appropriate filtering must be maintained to meet E-rate guidelines. Because filtering software is not 100% effective, 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 browser settings, and any other techniques designed to evade filtering or enable 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.

§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. Violation of copyright laws may expose the user, district, or school to legal action and/or financial penalties.

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. 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.

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

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

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

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

9.3.d. Unauthorized duplication of copyrighted material and/or use of such unauthorized material on state, district, or school equipment or networks is prohibited.

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

9.3.f. Employees will be provided yearly reminders of their responsibility through a district chosen procedure to adhere to and enforce the copyright laws and will be provided in-service training if necessary.

9.3.g. 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.

9.4. 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.

§126-41-10. Web Publishing.

10.1. The WVDE recommends that each district and/or school adopt local policies that are consistent with, but not limited to, the following web publishing guidelines:

10.1.a. Appropriate 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.b. 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/district server will take K-12 bandwidth 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, and districts/schools must respect parental refusals. Internet guidelines stress the importance of not publishing personally identifiable information of students.

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.

10.2.f. remain current, be accurate, and incorporate easy and user-friendly navigation through the site.

10.2.g. restrict business/commercial links or the acknowledgment of a business on a school/district web site to business partners and/or materials that are educational, provide technical support, or are germane to the educational mission of the school/district. Advertising commercial offerings is prohibited.

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

10.2.i. include the permission granted statement for all copyrighted materials.

10.2.j. complies with all W3C and ADA standards.

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

§126-41-11. Implementation.

11.1. Districts will ensure implementation of this policy by adopting their own district/school policies regarding acceptable use of electronic resources, technologies and the Internet.

11.2. The WVDE shall:

11.2.a. provide technical assistance to support districts, and schools in developing and implementing local use policies.

11.2.b. districts and schools with revisions of annual comprehensive technology plans associated with technology implementation and the West Virginia State Technology Plan.

§126-41-12. Severability.

12.1. 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.